

ValiCert[®] VA Publisher[™]

Installation and Administration Guide

Version 3.2



ValiCert[®]
Securing e-Transactions[™]

© 2000 ValiCert, Inc. All rights reserved. ValiCert and the ValiCert logo are registered trademarks of ValiCert, Inc. Powering e-Transactions, ValiCert Digital Receipt Solutions, ValiCert Enterprise VA Suite, ValiCert Enterprise VA, ValiCert Certificate VA Suite, ValiCert Certificate VA, ValiCert VA Publisher, ValiCert Validator Suite, ValiCert Web Server Validator, ValiCert E-Mail Validator, ValiCert Address Book Validator, ValiCert Browser Validator, ValiCert Validator Toolkit, ValiCert Receipt Notary, ValiCert Receipt Vault, ValiCert Receipt Toolkit, ValiCert SecureTransport, ValiCert SecureTransport/File, and ValiCert SecureTransport/XML and Stateful Validation are trademarks of ValiCert, Inc. ValiCert Global VA Service and ValiCert Receipt Service are service marks of ValiCert, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

ValiCert, Inc.
1215 Terra Bella Avenue
Mountain View, CA 94043

Part Number: DCU-B-VPiR-032E

Revision: 0100-1

Table of Contents

Preface

1 Introduction

Features	3
Supports Multiple CA Vendors	3
Publishes Data to Multiple Destinations Simultaneously	4
Supports Multiple Data Formats and Encodings	4
Supports Multiple Communication Protocols	5
Supports Multiple Modes of Operation	6
Provides Detailed Data Logging	6
Stores State Information	6
Supports SNMP	7
Operation	9
Modes of Operation	10
Continuous Mode	10
Command Line Mode	11
Command Line Arguments	11
Sample Command for Invoking VA Publisher	11
Triggered Mode	12
Configuration	12

2 Installing on Windows NT

Before you Begin	13
System Requirements for Windows NT	14
Pre-Installation Tasks for Windows NT	14

Upgrading to VA Publisher 3.2 on Windows NT	14
Upgrading from version 3.x on Windows NT	14
Installing the VA Publisher on Windows NT	17

3 Installing on UNIX

Before you Begin	33
System Requirements for UNIX	34
Pre-Installation Tasks	34
Upgrading VA Publisher on UNIX	34
Configuring for LDAP on UNIX	35
Configuring VA Publisher for Netscape CMS on UNIX	36
Installing the VA Publisher on UNIX	36
Obtaining the Installation Program (Solaris)	36
Installing from a CD	36
Installing VA Publisher (Solaris)	37
LDAP Installation Path	38
HTTPS Installation Path	39
HTTP Installation Path	40
FILE Installation Path	41

4 Using Certificate Servers

Netscape Certificate Server (CMS v.1.1)	44
Interface Modes for Fetching CRLs	44
Microsoft Certificate Server	46
Interface Mode for Fetching CRLs	46
Revoking a Certificate	46
Log File	47
Testing with Microsoft Certificate Server and Microsoft Outlook ...	47
Installing Microsoft Certificate Server Modules	47
VeriSign CA	47
Overview	47
Interface Modes for Fetching CRLs	48
CAs Using LDAP Directory Servers	48

LDAP Operation	49
File-Based CRL Repository	49
Fetching CRLs	50
Publishing CRLs	50
ValiCert VA	50
Publishing CRLs	50

5 Customizing the VA Publisher

Configuration File	51
Backward Compatibility	51
Syntax	51
Variables	52
Sample vpublish.ini File Before Editing	58
Sample Edited vpublish.ini File	64

A Testing and Troubleshooting

Testing Tools	65
Testing with SSLeay Tools	65
Testing the CRL Output	65
Verifying CRL Contents	66
Troubleshooting	67

B Using the SNMP Agent

Using SNMP with Windows NT	69
Requirements for NT	69
Installing the SNMP agent on Windows NT	70
Using SNMP with UNIX (Solaris)	71
Requirements	72
Installing Scotty	72
Running the SNMP Agent for UNIX	72
Configuring the SNMP Agent	72
Windows NT	72
UNIX (Solaris)	72
SNMP Variables	73
MIB Variables	73

Regular.....	73
Trap.....	75

Index

Preface

About This Guide

This guide describes the installation, configuration, and administration of the ValiCert VA Publisher.

Audience

This guide is intended for the ValiCert VA Publisher administrator and corporate security analysts.

The ValiCert VA Publisher administrator is defined as anyone responsible for installing, configuring, or maintaining the ValiCert VA Publisher.

We assume that the ValiCert VA Publisher administrator is any of the following:

- ❖ Customers with technical networking background and experience.
- ❖ System administrators familiar with the fundamentals of digital certificates and validation.
- ❖ System administrators responsible for installing and configuring software packages.

Organization of This Guide

This guide is organized as follows:

Section	Description
Introduction	Provides an introduction to the product.
Installing on Windows NT	Demonstrates how to perform a default installation of the product on a Windows NT workstation/server.
Installing on UNIX	Demonstrates how to perform a default installation of the product on a Sun workstation running Solaris.
Using Certificate Servers	Explains the operation of the software with a variety of certificate management systems.
Customizing the VA Publisher	Provides information about configuring input and output locations, protocols and encodings in the VA Publisher ini files.
Testing and Troubleshooting	Reviews VA Publisher operational testing using SSLeay, Global VA Service, Enterprise VA, and MS Certificate Server, and provides troubleshooting information.

Typographical Conventions

The following typographical conventions are used in this guide to help you locate and identify information:

Italic text is used for emphasis and book titles.

Bold text identifies menu names, menu options, items you can click on the screen, and keyboard keys.

`Courier font` identifies commands you enter at the command line, file names, folder names, code, and text that either appears on the screen or that you are required to type in.



NOTE: Notes provide significant, helpful information about a feature, operation, or procedure.

Abbreviations and Acronyms

The following terms are used in this manual, or are related to topics covered in this guide:

Abbreviation/ Acronym	Definition
CA	Certificate Authority, an entity that issues certificates
CRL	certificate revocation list, a list of revoked certificates
CRL-DP	CRL distribution points, geographically or functionally localized CRLs
CRT	Certificate Revocation Tree
DN	Distinguished Name, a unique naming scheme
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
S/MIME	Secure MIME
SHA-1	Secure Hash Algorithm
SSL	Secure Sockets Layer
VA	Validation Authority
X.509	internationally recognized electronic document used to prove identity and public key ownership over a communication network

ValiCert Documentation

- ❖ ValiCert Enterprise VA™ Installation and Administration Guide
- ❖ ValiCert VA Publisher™ Installation and Administration Guide
- ❖ ValiCert Validator Suite™ Installation and Configuration Guide
- ❖ ValiCert Validator Toolkit™ Programmer's Guide

Technical Support

ValiCert provides debugging assistance, integration assistance and general customer support. Please contact us through one of the following methods:

- ❖ Email: support@valicert.com
- ❖ Telephone: +1.650.567.5469
- ❖ Fax: +1.650.254.2148

When you contact us, we would appreciate your sending us as much detailed information as possible regarding your:

- ❖ Network
- ❖ Platform
- ❖ Specific problem and how to reproduce it.

Credits

This product contains encryption software from RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. All Rights Reserved.



This product includes portions of SSLeay software written by Eric Young (eyay@mincom.oz.au). Copyright (C) 1995-1997 Eric Young. All rights reserved. This product includes software written by Tim Hudson (tjh@mincom.oz.au).



This product includes software from Netscape Communications Corp. Copyright (C) 1997 Netscape Communications Corp. All rights reserved.



Introduction

The ValiCert VA Publisher is an application which retrieves (fetches) certificate revocation data (typically a CRL), and sends (publishes) it to one or more destinations.

VA Publisher supports input from multiple data sources, can publish to multiple destinations, and can use different communication protocols.

VA Publisher transports Certificate Authority (CA) specific revocation data. The types of input data are:

- ❖ Full CRLs
- ❖ X.509 Certificates
- ❖ CRLDPs

VA Publisher fetches these data types from various sources like third-party vendor Certificate Authority software packages. The same VA Publisher can fetch data from multiple sources, including CAs and LDAP servers.

VA Publisher publishes the revocation data to one or more destinations. These destinations are typically:

- ❖ ValiCert Validation Authorities
- ❖ ValiCert Global VA Service
- ❖ LDAP Servers

VA Publisher can publish all retrieved data, or subsets of the retrieved data. The source data each destination receives is configured separately within VA Publisher.

VA Publisher can store state information about the revocation data that it receives. This allows VA publisher to avoid publishing redundant CRL data. VA publisher also stores state information about fetch and publish requests. In cases where requests are denied, because the source or the destination is temporarily unavailable, Publisher can be configured to retry the requests.

The VA Publisher acts like a smart information hub.

- ❖ It fetches data individually from members of a set of different sources (at time intervals configured individually for each source).
- ❖ It combines the data from different members of the data sources set to create subsets of the total data input.
- ❖ It publishes the subsets of data to specific destinations (at time intervals configured individually for each destination).
- ❖ It stores state information for the revocation data that it fetches and for the fetch and publish requests themselves.

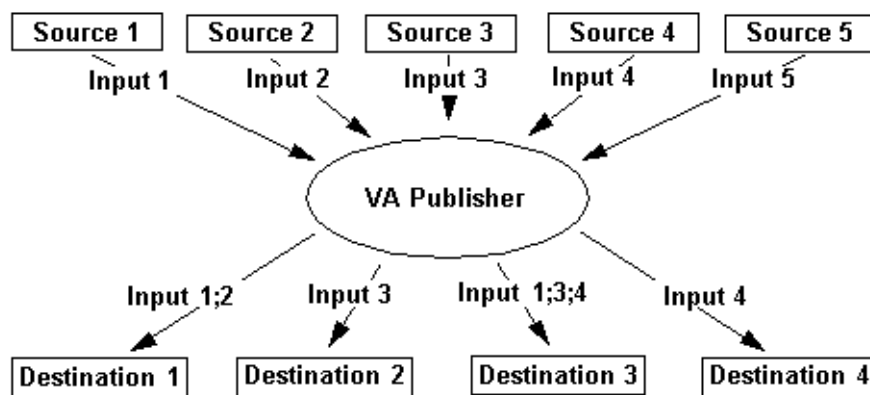


Figure 1 Data Distribution Topology (Multiple Data Sources and Destinations)

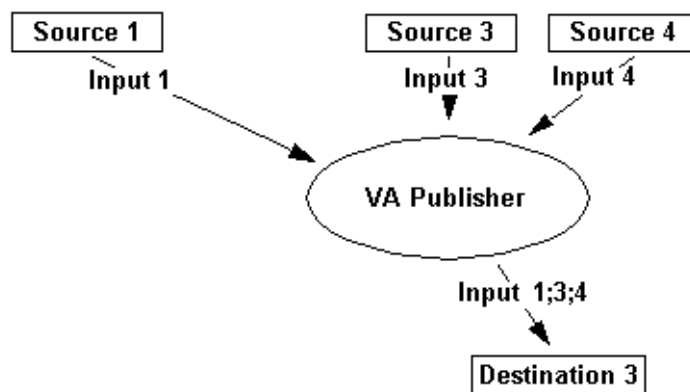


Figure 2 Data from Multiple Sources Published to One Destination

Features

The VA Publisher:

- ❖ Supports Multiple CA Vendors
- ❖ Publishes Data to Multiple Destinations Simultaneously
- ❖ Supports Multiple Data Formats and Encodings
- ❖ Supports Multiple Communication Protocols
- ❖ Supports Multiple Modes of Operation, including operation as a service
- ❖ Provides Detailed Data Logging
- ❖ Stores State information for requests and for CRLs
- ❖ Supports the Simple Network Management Protocol (SNMP) and provides an SNMP agent

Supports Multiple CA Vendors

VA Publisher can retrieve information from multiple types of sources, simultaneously including multiple CA vendors. Each source can have its own distinct data type. The data source addresses, and associated source types, are configured in the `vpublish.ini` file.

The VA Publisher retrieves data from the following source types:

- ❖ Microsoft CA
- ❖ VeriSign Onsite CA
- ❖ Netscape CA
- ❖ CAs that store CRLs in LDAP directories (such as Entrust PKI, GTE, and Baltimore UniCERT)
- ❖ All other CAs which support HTTP/HTTPS generic protocols
- ❖ Validation Authorities (ValiCert Enterprise VA, ValiCert Global VA Service)
- ❖ LDAP Directory

- ❖ File

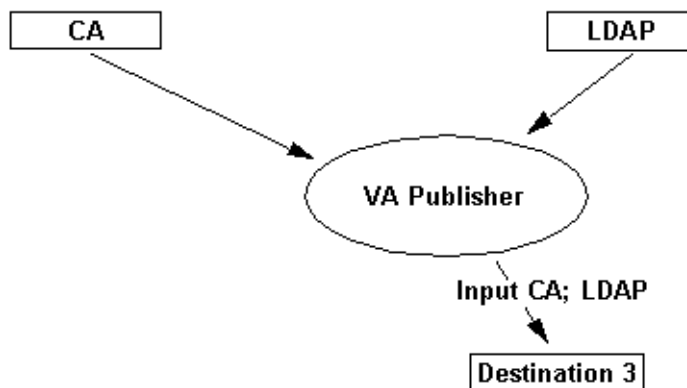


Figure 3 Multiple Data Sources with Multiple Data Types

Publishes Data to Multiple Destinations Simultaneously

VA Publisher publishes data to multiple destinations, including:

- ❖ Validation Authorities (like the ValiCert Enterprise VA and the ValiCert Global VA Service)
- ❖ LDAP Directories
- ❖ Files

Supports Multiple Data Formats and Encodings

The VA Publisher handles multiple data sources and multiple data destinations running at the same time. Data formats and encodings are specified in the configuration file. Each data source, and data destination is configured individually.

The VA Publisher supports the following standard data formats:

- ❖ CRL (Full CRL, CRLDP)
- ❖ PKCS7

- ❖ X.509 Certificate



NOTE: The convention in this manual is to use the term CRL as a general term, in place of any data formats supported by VA Publisher.

The VA Publisher supports the following standard encodings:

- ❖ DER
- ❖ HEX
- ❖ Base64

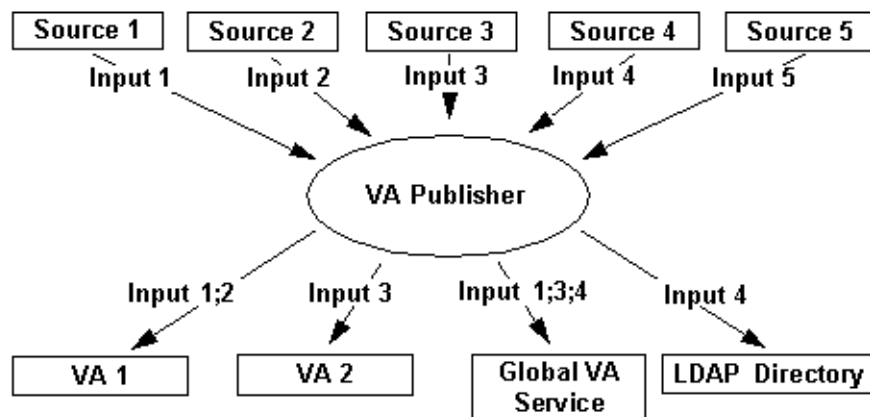


Figure 4 Multiple Data Destinations

Supports Multiple Communication Protocols

The VA Publisher handles the following standard protocols for fetching data:

- ❖ LDAP—Any CA using an LDAP directory for storing CRLs (for example, Entrust/PKI, Entegrit, Netscape CMS 4.x, GTE CyberTrust, Baltimore UniCERT with LDAP directory)
- ❖ HTTP—for example, VeriSign OnSite
- ❖ HTTPS—for example, Netscape Certificate Server v1.x
- ❖ COM Interface—for example, Microsoft Certificate Server or Windows 2000 CA (native code which uses the COM interface)

- ❖ **FILE**—Read from a file (for example, Baltimore UniCERT, or any CA using a file for storing CRLs)

Supports Multiple Modes of Operation

VA Publisher can operate in multiple modes, including as a service/daemon. The interval between data fetches can be configured independently for each data source. This interval between data fetches is called the periodicity. For more information, see “Modes of Operation” on page 10.

Provides Detailed Data Logging

All significant VA Publisher ‘events’ can be written to a file. The default log file name is `vpublish.log` (specified in the configuration file, `vpublish.ini`).

If the default log file is specified, all log messages are written to that file. If you do not specify a default log name, logs are created and are rolled over each time the log reaches a configured size. The name of each of these log files contains a time stamp and the prefix specified in the `ini` file (default is `pub`).

The level of detail for data logging is specified in the `ini` file. The supported logging levels are as follows:

- ❖ **Debug level**, which provides descriptive diagnostics
- ❖ **Brief logging entries**

For more information, see the logging variable descriptions in Chapter 5, “Customizing the VA Publisher.”

Stores State Information

VA publisher stores state information for requests (fetch and publish) as well as for the revocation data that is fetched. This allows VA Publisher to:

- ❖ **Avoid redundant publishing of CRL data**
- ❖ **Schedule the next data fetch for the next time the data is updated**
- ❖ **Re-attempt to fetch revocation data from a source that was unavailable**
- ❖ **Re-attempt to publish revocation data to a source that was unavailable**

The state information for revocation data is only stored for CRLs. This also includes CRLs stored in a PKCS7 object. The CRL is the full CRL or the CRLDP.

To maintain state information, VA Publisher stores `.state` files in subdirectories (`/source` and `/dest`) of the installation directory. For the

source information the CRL (.crl) is stored as well as any certificates (.crt). If the VA Publisher is restarted, it reads the state information files. If the files are not present, VA Publisher creates them.

Supports SNMP

VA Publisher supports the Simple Network Management Protocol (SNMP) and provides an SNMP agent to help you monitor the VA Publisher through an SNMP Manager such as Hewlett Packard OpenView or IBM Tivoli. The Manager requests and gets error information from the MIB at configured time intervals or receives traps (unsolicited error information) when a pre-defined triggering event occurs. The MIB is maintained by the SNMP Agent.



NOTE: Although the ValiCert SNMP Agent runs as a separate process from the VA Publisher, they must be installed on the same host.

Figure 5 shows the relationship between VA Publisher, the ValiCert SNMP Agent, and the SNMP Manager.

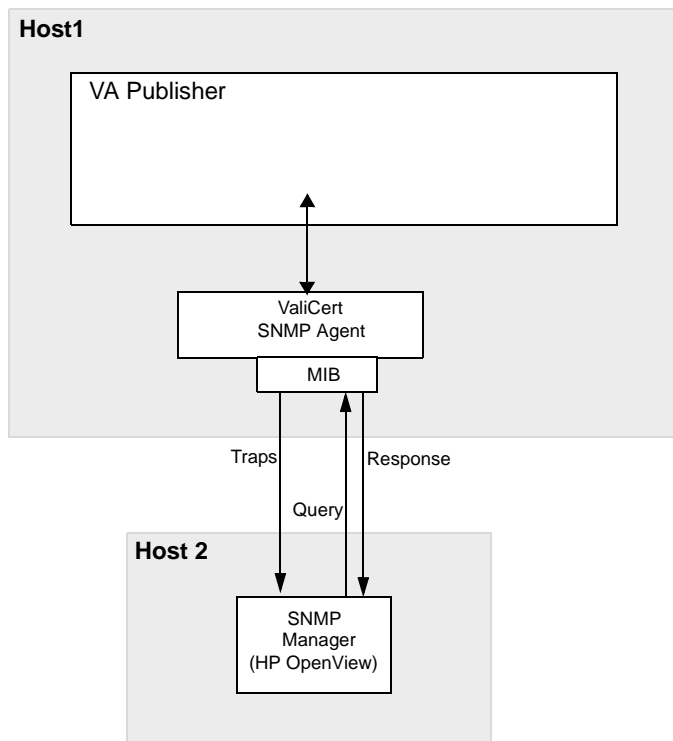


Figure 5 SNMP Support Overview

The SNMP Agent periodically updates the MIB variables. The SNMP Manager sends a query to the SNMP agent (performs a GET or GETNEXT SNMP operation) to read the current values of the MIB variables. MIB variables are maintained in the ValiCert MIB. The Manager displays this information at its user interface.

If the SNMP Agent discovers that a trap-triggering event has occurred (the Publisher is down), it updates the corresponding MIB variable instance and sends a trap message to the SNMP Manager. Traps are sent automatically, the SNMP Manager does not request this information. Once the SNMP Manager receives a trap message it can alert the user. How the user is alerted is also configurable (through the Manager).

The information the SNMP Agent tracks is as follows:

- ❖ Service/daemon health (a trap is available to alert the user if the Service/Daemon is down)
- ❖ Service/daemon state information
- ❖ Service error/warning information
- ❖ Service/daemon Up/Down status

Operation

A CA issues CRLs. The VA Publisher fetches the newly generated CRL and can publish it to each of the following Validation Authority servers or to any LDAP directory:

- ❖ ValiCert Enterprise VA™
- ❖ ValiCert Certificate VA™
- ❖ ValiCert Global VA ServiceSM
- ❖ LDAP Directory

Figure 6 shows the architecture for using the VA Publisher directly with a certificate server.

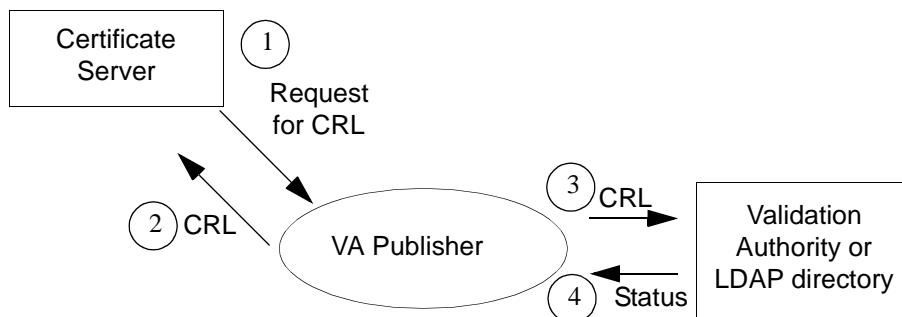


Figure 6 VA Publisher—Direct Interface with a Certificate Server

Figure 7 shows the architecture for using the VA Publisher with an LDAP server.

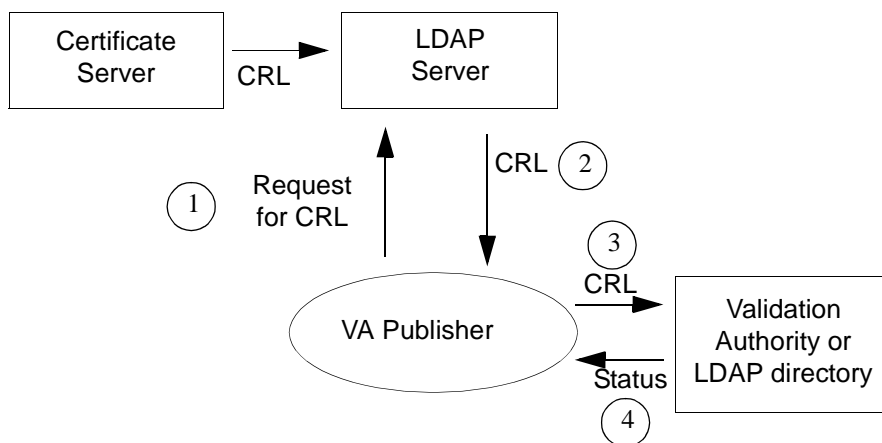


Figure 7 VA Publisher—Direct Interface with an LDAP Server

Modes of Operation

The VA Publisher retrieves data based on the mode in which it is operating. The VA Publisher can operate in the following modes:

- ❖ Continuous Mode—Run continuously, usually a service/daemon
- ❖ Command Line Mode—Run from the command line
- ❖ Triggered Mode—Certificate Authority triggers VA Publisher



NOTE: Do not invoke the VA Publisher at the same time that it is running in service mode.

Continuous Mode

In this mode, the VA Publisher runs continuously in the background, similarly to a Windows NT service, or a UNIX daemon. In continuous mode, VA Publisher reads data from one or more sources, at specific time intervals. The

time intervals are either configured the same for all sources (default condition), or specified for each source independently.

Command Line Mode

When the VA Publisher is run from the command line, it retrieves the data, publishes it to the destinations, returns an exit code and exits. Exit codes are:

- ❖ 0—successful invocation of VA Publisher
- ❖ 1—failure to get a CRL or Certificate and publish the data to the destination (VA or LDAP)

The UNIX version of the VA Publisher program is called `vpublish`. Under Windows NT, the program is called `vpublish.exe`. On both platforms, the program may be invoked from a shell command line.

Command Line Arguments

The following table summarizes VA Publisher command line arguments, their purpose and default values.

Table 1. VA Publisher Command Line Arguments

Argument	Purpose	Default
<code>-c configfilename</code>	Uses the specified file for the configuration.	<code>./vpublish.ini</code> .
<code>-v</code>	Prints the VA Publisher version number and the list of supported CA servers to the <code>stdout</code> then exits.	Does not print this information to <code>stdout</code> .
<code>+name=value</code>	Assigns the value to the named configuration variable.	Configuration variable value set elsewhere.
<code>-service</code>	Runs VA Publisher as a service.	Disabled.

Sample Command for Invoking VA Publisher

To invoke the VA Publisher use a command line similar to the following:

```
Prompt> vpublish -c foo.ini +VC_LOG_FILE=foo.log
```

For information on command line options, see the Configuration section within this chapter.

Triggered Mode

A certificate server may trigger the VA Publisher. The CA updates data and notifies the VA Publisher that there is new data. VA Publisher retrieves the data and publishes it to the appropriate destinations.

Configuration

The VA Publisher is highly configurable. It uses a simple name/value pair configuration mechanism that is a variant of the Windows configuration file. To configure the VA Publisher, edit the `ini` file, or enter a command line option.

The VA Publisher acquires its configuration in the following order:

- 1 It reads the configuration file. The default configuration file is called `vpublish.ini`. To specify a different file name use the `-c` flag on the command line.
- 2 It obtains any configuration settings from the command line. Configuration variables are specified with the syntax `PARAMETER = value`.

In all cases, a configuration variable assignment made in a later stage overwrites a previous assignment.

A complete list of configuration variables and the precise configuration syntax is provided in Chapter 5, "Customizing the VA Publisher."

Installing on Windows NT

This section describes how to install your ValiCert VA Publisher on a Windows NT server or Windows NT workstation. It describes:

- ❖ System requirements and pre-installation tasks that you must complete before you install
- ❖ How to upgrade to VA Publisher 3.2
- ❖ How to install VA Publisher 3.2

For information on how to install the VA Publisher on a UNIX platform, see Chapter 3, "Installing on UNIX."

Before you Begin

Before you begin installing the ValiCert VA Publisher, be sure that the following requirements are met:

- ❖ System Requirements for Windows NT
- ❖ Pre-Installation Tasks for Windows NT

Once the requirements are met, continue with one of the following procedures:

- ❖ Upgrading to VA Publisher 3.2 on Windows NT
- ❖ Installing the VA Publisher on Windows NT

System Requirements for Windows NT

Table 2 lists the requirements for VA Publisher on a Windows NT server and Windows NT workstation.

Table 2. System Requirements on Windows NT

Item	Native Interface
Hardware	Minimum: Intel 166 MHz Pentium-based or compatible systems. Recommended: Intel 300MHz Pentium-II based or compatible systems.
Memory	Minimum: 32 MB Recommended: 64 MB
Disk Space	Minimum: 20 MB
Operating System	Windows NT Workstation 4.0 or Windows NT Server 4.0 or later (both with service pack 3, 5, or later).

Pre-Installation Tasks for Windows NT

- ❖ Be sure that you have administrative privileges on the machine where you plan to install the VA Publisher.
- ❖ If you are using Netscape Certificate Server v.1.1 or Netscape Certificate Management System (CMS) 4.1, install VA Publisher on the same machine as the CA server.
- ❖ Make sure you have administrative privileges to start and stop the Certificate Server.

Upgrading to VA Publisher 3.2 on Windows NT

You can upgrade your VA Publisher from a previous version to version 3.2. For versions 3 and higher, the installer automatically backs up the current installation and upgrades the Publisher.

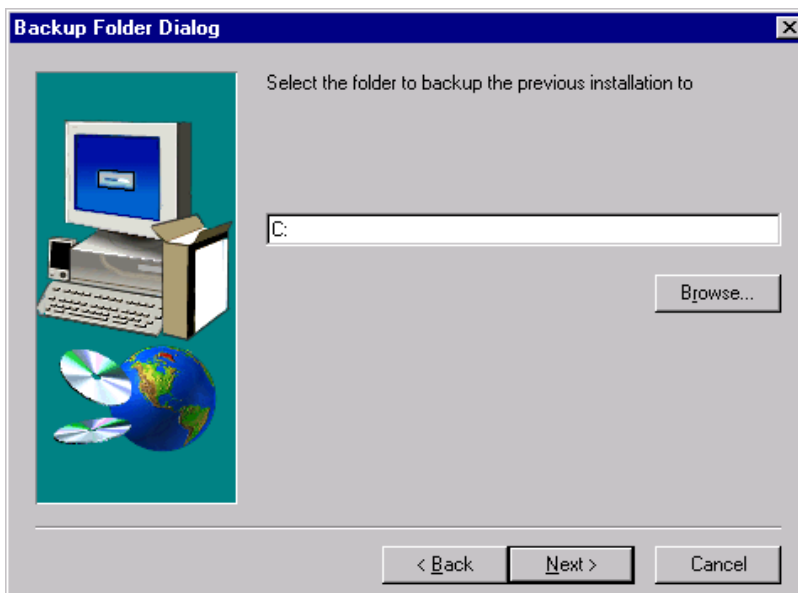
Upgrading from version 3.x on Windows NT

To upgrade VA Publisher from a version run the install program.

To upgrade the ValiCert VA Publisher on Windows NT

- Step 1 Insert the CD into the CD drive on your intended VA Publisher server.
- Step 2 Double click on the self-extracting file Publisher32Setup.
- Step 3 The Installation Folder dialog box displays.
Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.
- Step 4 Click **Finish**.
- Step 5 The installation files are unpacked and the Setup.exe program launches.
A dialog displays asking if you want to upgrade.
- Step 6 Click **Yes** to upgrade.
The welcome dialog displays.
- Step 7 Click **Next**.
The Software License Agreement displays.
- Step 8 Click **Yes**.

The previous Publisher is stopped. The Backup Folder dialog box displays.



Step 9 Accept the default folder or browse to a desired folder.

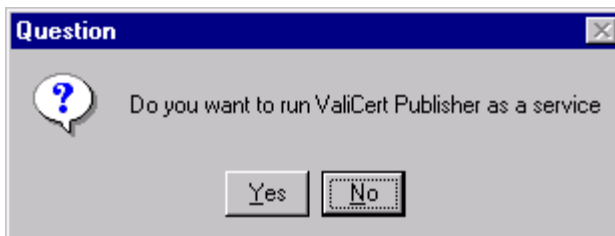
Step 10 Click **Next**.

A dialog displays informing you the files are backed up.

Step 11 Click **OK**.

The software installs.

The run Publisher as a Service question dialog displays:



Step 12 Click **Yes** or **No**.

The setup is complete.

Installing the VA Publisher on Windows NT

This section describes how to install the VA Publisher on the Windows NT platform. Be sure that your system meets the system requirements and that you have completed the pre-installation tasks described in “Before you Begin” on page 13.

To install the VA Publisher follow the instructions below:

The VA Publisher is distributed on a CD. Install it from the CD.

To install VA Publisher from a CD

- Step 1 Insert the CD into the CD drive on your intended VA Publisher server.
- Step 2 Double click on the self-extracting file Publisher32Setup.
- Step 3 The Installation Folder dialog box displays.
Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.
- Step 4 Click **Finish**.
- Step 5 The installation files are unpacked and the Setup.exe program launches.

The Install Shield application starts and the Welcome dialog box displays:



Follow the on-screen instructions as you proceed through the installation.

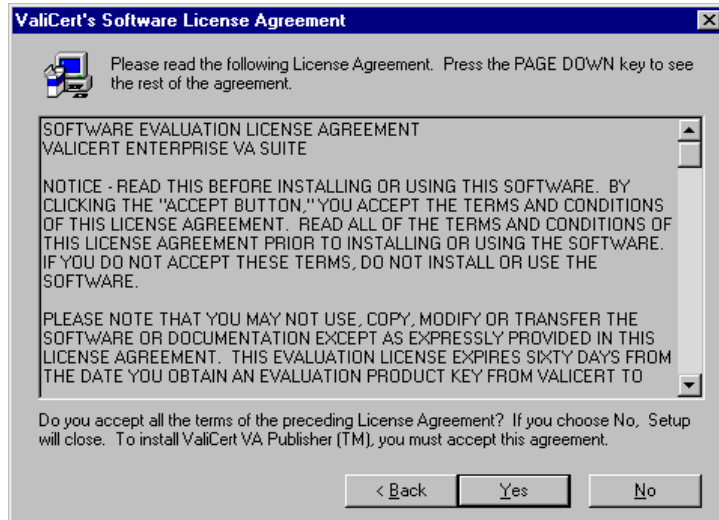
The **Next** button allows you to move forward to the next installation window.

The **Back** button allows you to return to the previous installation window

The **Cancel** button closes the installation program without installing any component of the Validator suite. To install Publisher, rerun the installation program.

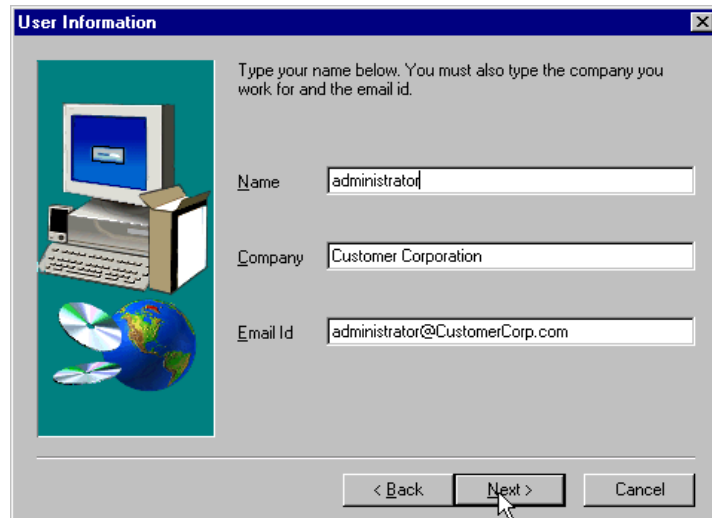
Step 6 Click **Next**.

The ValiCert Software License Agreement dialog box displays:



Step 7 Click **Yes** to accept the license agreement.

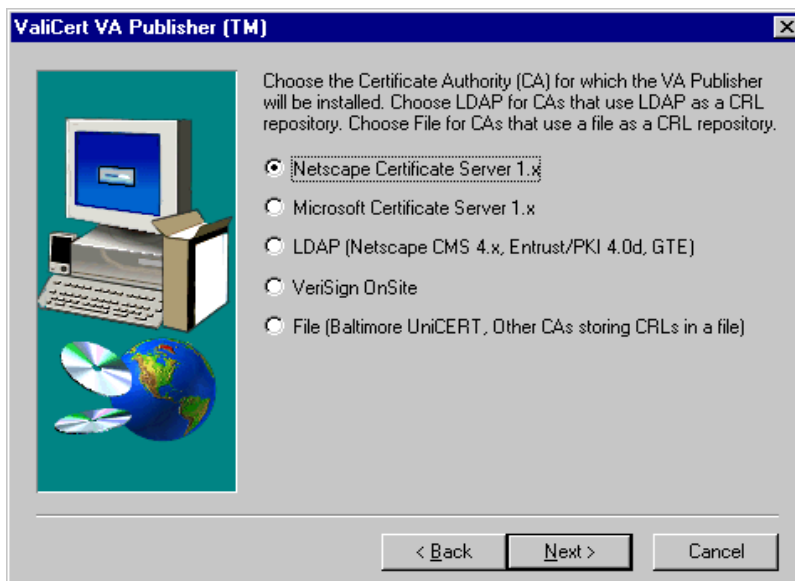
The User Information dialog box displays:



Step 8 Type your **Name**, **Company** and **Email ID** (email address) in the text fields provided.

Step 9 Click **Next**.

The following dialog box displays:



Step 10 Select the option that is appropriate for the type of CA you are using.



NOTE: This is a branch point in the installation process.

You can select one of the following options:

Netscape Certificate Server

Microsoft Certificate Server

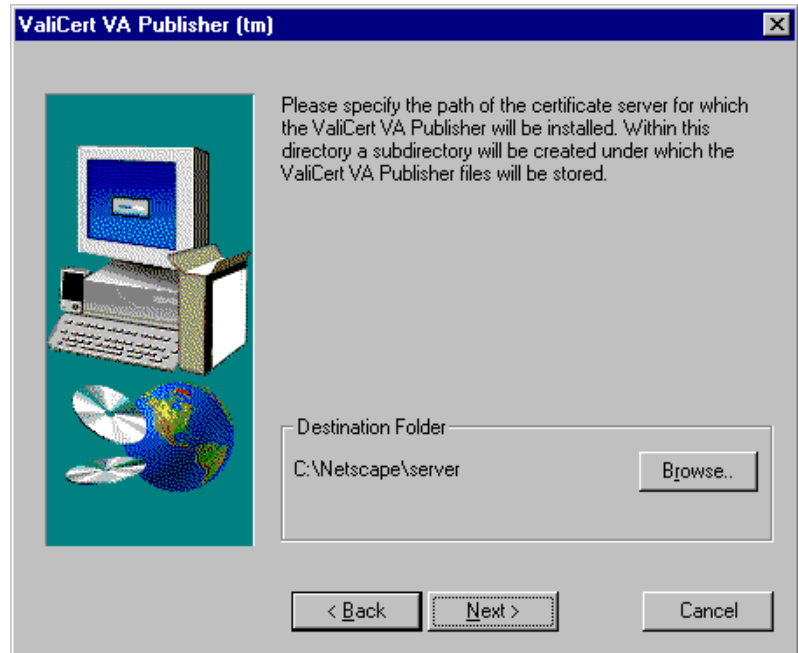
LDAP (Netscape CMS 4.x, Entrust/PKI 4.0d, or GTE)

VeriSign OnSite CA

File (Baltimore UniCERT, Other CAs storing CRLs in a file)

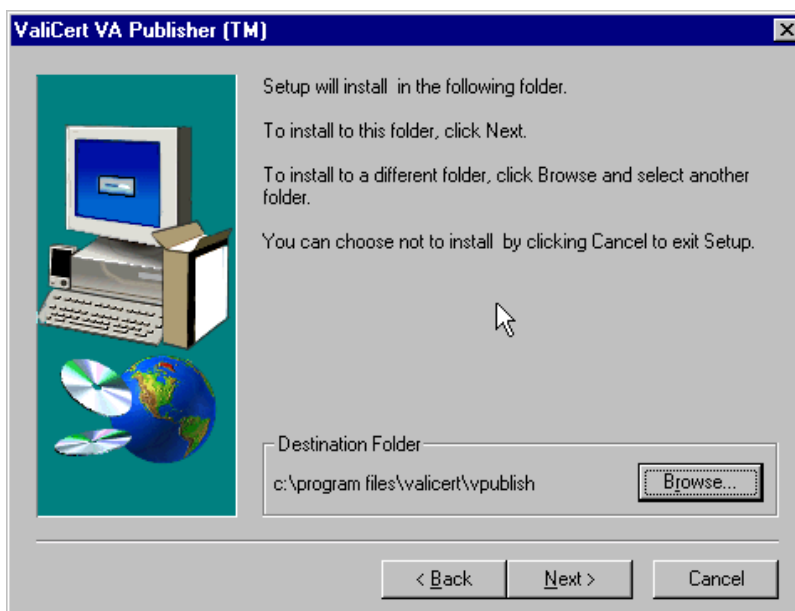
Step 11 Click **Next**.

If you selected Netscape Certificate Server, the following Destination Folder dialog box displays:



OR

If you selected any of the other options, the following Destination Folder dialog box displays:



If you selected **Netscape Certificate Server** option, continue with step 12.

If you selected the **Microsoft Certificate Server** option, skip to step 13.

If you selected the **LDAP (Netscape CMS 4.x, Entrust/PKI 4.0d, or GTE)** option, skip to step 14.

If you selected the **VeriSign OnSite CA** option, skip to step 15.

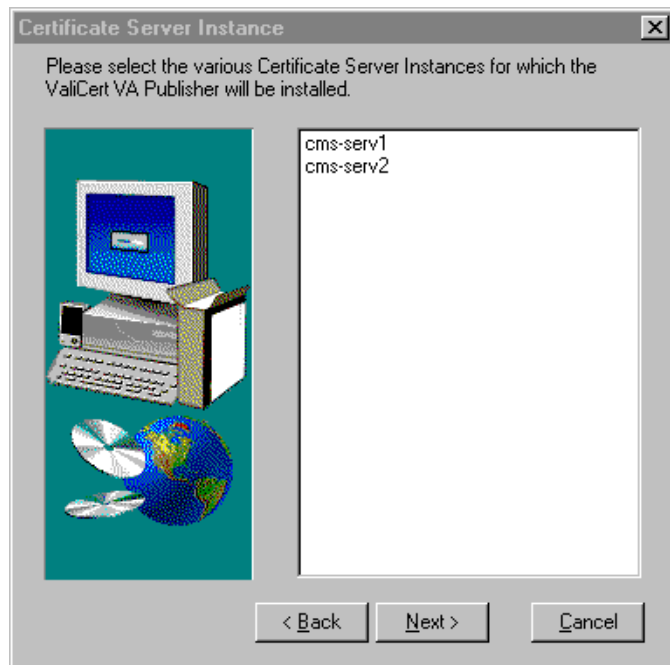
If you selected the **File (Baltimore UniCERT, Other CAs storing CRLs in a file)** option, skip to step 16.

Step 12 For the **Netscape Certificate Server** option, specify the path to the Netscape Certificate Server.

Use the **Browse** button, if necessary, to navigate to the directory containing the certificate server.

a Click **Next**.

The Certificate Server Instance dialog box displays:



- b Click on an instance in the list box. Control-click if you are selecting more than one instance.

Proceed to step 17.

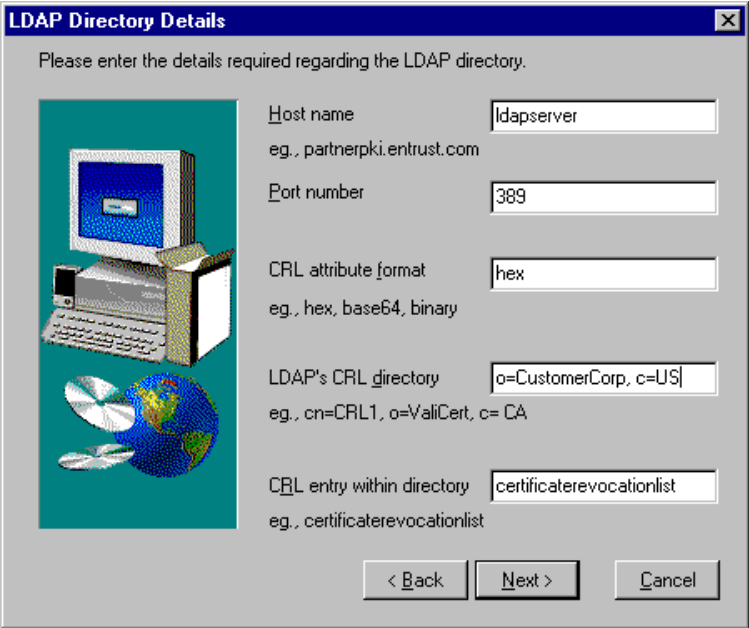
- Step 13 For the **Microsoft Certificate Server** option, use the default path where the VA Publisher will be installed or use the **Browse** button, if necessary, to navigate to a different folder.

Proceed to step 17

- Step 14 For the **LDAP (Netscape CMS 4.x, Entrust/PKI 4.0d, or GTE)** option, use the default path where the VA Publisher will be installed or use the **Browse** button, if necessary, to navigate to a different folder.

- a Click **Next**.

The LDAP Directory Details dialog box displays:



LDAP Directory Details

Please enter the details required regarding the LDAP directory.

Host name: ldapservers
eg., partnerpki.entrust.com

Port number: 389

CRL attribute format: hex
eg., hex, base64, binary

LDAP's CRL directory: o=CustomerCorp, c=US
eg., cn=CRL1, o=ValiCert, c=CA

CRL entry within directory: certificaterevocationlist
eg., certificaterevocationlist

< Back Next > Cancel

b Type the appropriate information in the text fields.

Host Name—for the LDAP Directory

Port Number—for the LDAP Directory

CRL Attribute Format—allowable values are *hex*, *base64* or *binary*

LDAP's CRL Directory—the DN where the CRL is located

CRL Entry within the Directory

Proceed to step 17.

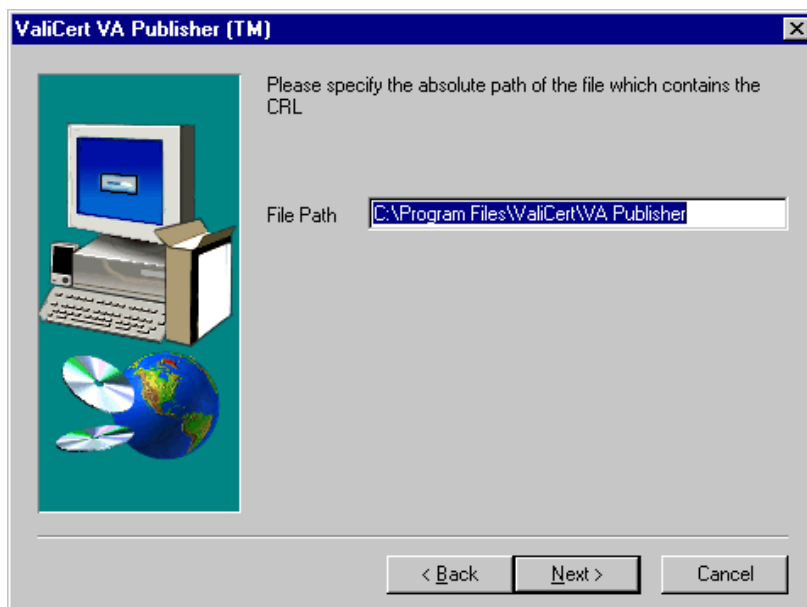
Step 15 For the **VeriSign OnSite CA** option, use the default path where the VA Publisher will be installed or use the **Browse** button, if necessary, to navigate to a different folder.

Proceed to step 17

Step 16 For the **File** option (**Baltimore UniCERT, Other CAs storing CRLs in a file**), use the default path where the VA Publisher will be installed or use the **Browse** button, if necessary, to navigate to a different folder.

a Click **Next**.

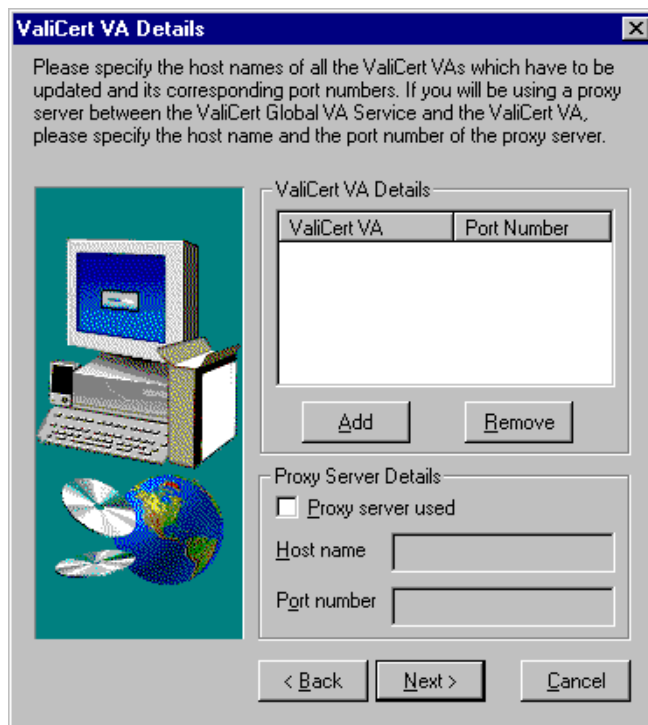
The File Path dialog box displays:



- b Type the absolute path of the file that contains the CRL.
Proceed to step 17.

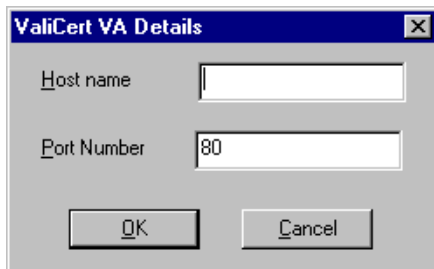
Step 17 Click **Next**.

The ValiCert VA Details dialog box displays:



Step 18 Click **Add**.

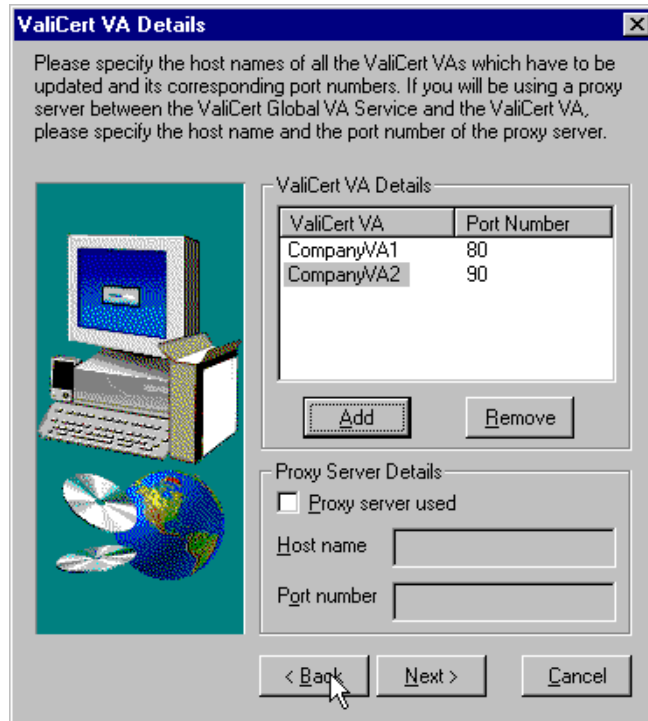
The ValiCert VA Details dialog box displays:



Step 19 Type the **Host Name** and the **Port Number** for a ValiCert Enterprise VA/ValiCert Certificate VA that is the destination for the VA Publisher's CRLs.

Step 20 Click **OK**.

Repeat steps 14 through 16 until you have added all of the ValiCert VAs. All the ValiCert VA **Host names** are now contained in the list box.



The dialog box titled "ValiCert VA Details" contains instructions at the top: "Please specify the host names of all the ValiCert VAs which have to be updated and its corresponding port numbers. If you will be using a proxy server between the ValiCert Global VA Service and the ValiCert VA, please specify the host name and the port number of the proxy server."

On the left is a graphic of a computer monitor, keyboard, and CD-ROMs. On the right is a table titled "ValiCert VA Details":

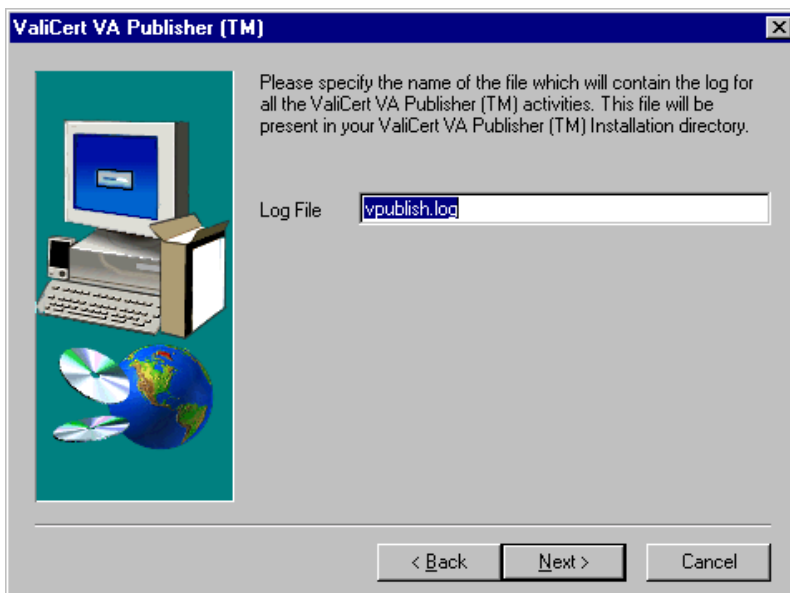
ValiCert VA	Port Number
CompanyVA1	80
CompanyVA2	90

Below the table are "Add" and "Remove" buttons. Under the heading "Proxy Server Details", there is a checkbox labeled "Proxy server used" which is currently unchecked. Below this are text input fields for "Host name" and "Port number". At the bottom are "< Back", "Next >", and "Cancel" buttons. A mouse cursor is pointing at the "< Back" button.

Step 21 Select the **Proxy server used** checkbox to use a proxy server to communicate to the ValiCert Enterprise VA or ValiCert Certificate VA. Type the server's **Host Name** and **Port Number** in the appropriate text fields.

Step 22 Click **Next**.

The Log File dialog box displays:

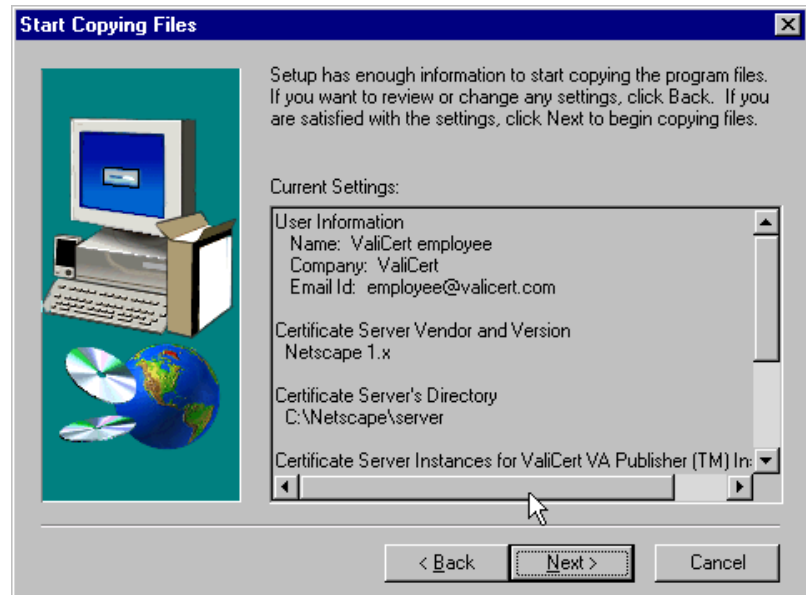


Step 23 Type the full path for the VA Publisher log file.

The default file name is `vpublish.log` and the default location is your installation directory.

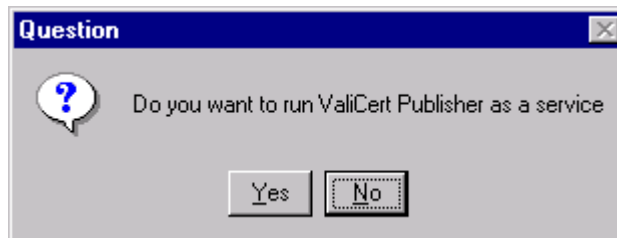
Step 24 Click **Next**.

The Start Copying Files dialog box displays:



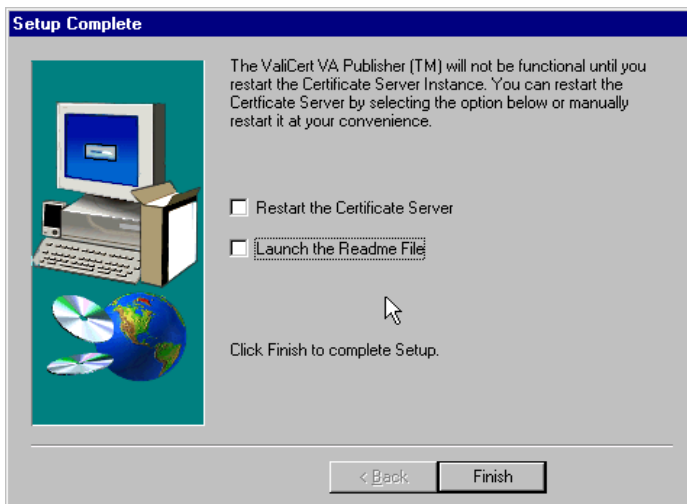
Step 25 Click **Next**.

The Publisher installs and the run Publisher as a Service question dialog displays:



Step 26 Click **Yes** or **No**.

For the **Netscape Certificate Server** and **Microsoft Certificate Server** options, the Setup Complete dialog box displays:



- a Select whether to restart the Certificate Server immediately after setup completes.
- b Select whether you want to launch the Read me file.

For the **LDAP (Netscape CMS 4.x, Entrust/PKI 4.0d, GTE)**, **VeriSign OnSite CA**, and **File (Baltimore UniCERT, Other CA**

storing CRLs in a File) options, the following Setup Complete dialog box displays:



a Select whether you want to launch the Read me file.

Step 27 Click **Finish**.

Installation is complete.



NOTE: Restart the CA for the configuration changes of the CA to take effect.

After VA Publisher is installed, edit the `vpublish.ini` file (present in your installation directory) to change any of these settings.

Installing on UNIX

This section describes how to install your ValiCert VA Publisher on a Sun Sparc Station running the Solaris operating system. It describes:

- ❖ System requirements and pre-installation tasks that you must complete before you install VA Publisher software
- ❖ How to upgrade from VA Publisher 2.0 to 3.2
- ❖ How to install VA Publisher 3.2

For information about installing the VA Publisher on a Windows NT platform, see Chapter 2, "Installing on Windows NT."

Before you Begin

Before you install the ValiCert VA Publisher:

- ❖ Check the System Requirements for UNIX
- ❖ Complete the Pre-Installation Tasks

Once you have completed tasks, you can continue with one of the following procedures:

- ❖ Upgrading VA Publisher on UNIX
- ❖ Installing the VA Publisher on UNIX

System Requirements for UNIX

Table 3 provides the requirements for a Sun Workstation running VA Publisher.

Table 3. System Requirements for UNIX

Item	Native Interface
Hardware	Minimum: Sun SPARC-based workstation.
Memory	Minimum: 64 MB
Disk Space	Minimum: 60 MB
Operating System	Solaris 2.6/2.7

Pre-Installation Tasks

Before you install any software:

- ❖ Be sure that you have root privileges on the machine where you plan to install the server.
- ❖ Be sure that the VA Publisher will be installed on the same machine as the third-party publisher you are using.
- ❖ Be sure that you have the administrative privileges to start and stop the certificate server.
- ❖ Determine whether this is a new installation or an upgrade.

Upgrading VA Publisher on UNIX

You can upgrade your VA Publisher from a previous version to version 3.2. In addition to the upgrade procedure, you may need to configure the VA Publisher with values from your previous configuration file. Use the following procedures to copy previous configurations during the re-installation:

- ❖ Configuring for LDAP on UNIX
- ❖ Configuring VA Publisher for Netscape CMS on UNIX

To upgrade to VA Publisher 3.2

Back up the configuration (*ini*) file, remove the previous installation, install the new application and configure it using the backed up *ini* file. You can configure the Publisher during the installation part of the process or you can configure it after.

Step 1 Backup the `vpublish.ini` file from your ValiCert VA Publisher installation.

The `vpublish.ini` file stores configuration information for the ValiCert VA Publisher.

Step 2 Uninstall VA Publisher.

To remove the current ValiCert VA Publisher installation, on a shell command-line, type:

```
pkgrm VCRTpub
```

Step 3 Install ValiCert VA Publisher 3.2. Use the `vpublish.ini` file to reply to the prompts during the installation,

Refer to “Installing the VA Publisher on UNIX” on page 36 for detailed installation instructions.

Step 4 Configure the ValiCert VA Publisher 3.2 using the information that is present in the `vpublish.ini` that you had backed up in Step 1.

Configuring for LDAP on UNIX

To configure the VA Publisher for LDAP on UNIX, use the backed up `vpublish.ini` file. To use the configuration variables from the previous install, enter the following values when prompted during the install script:

To configure VA Publisher for LDAP on UNIX

Step 1 Enter the value of `LDAP_SERVER` in the `vpublish.ini` file as the name of the LDAP server

Step 2 Enter the value of `LDAP_CRL_ATTRIBUTE_FORMAT` in the `vpublish.ini` file as the encoding of the CRL.

Step 3 Enter the value of `LDAP_CRL_DN` in the `vpublish.ini` file as the DN containing the CRL

Step 4 Enter the value of `LDAP_CRL_ATTRIBUTE` in the `vpublish.ini` file as the attribute for the CRL.

Step 5 Enter the value of `LDAP_PORT` in the `ini` file as the LDAP server's port number.

- Step 6 Enter the values of variables in the `VVS_LOCATION` as the name and port of the validation server(s).

Configuring VA Publisher for Netscape CMS on UNIX

To configure the VA Publisher for Netscape Certificate Management System 1.01, use the backed up `vpublish.ini` file. To use the configuration variables from the previous install, enter the following values when prompted during the install script:

To configure VA Publisher for Netscape CMS on UNIX

- Step 1 Choose the Certificate Server Instance that is specified in the `vpublish.ini` file as the value of variable `SERVER_NAME`.
- Step 2 Enter the value of variable `SERVER_PORT` as the port number for the Certificate Server Instance.
- Step 3 Enter the values of variables in the `VVS_LOCATION` as the name and port of the validation server(s).

Installing the VA Publisher on UNIX

Before you install the ValiCert VA Publisher, ensure that your system has met the system requirements and perform the pre-installation tasks described in “Before you Begin” on page 33.

Installing the VA Publisher is described as two separate tasks:

- ❖ Obtaining the Installation Program (Solaris)
- ❖ Installing VA Publisher (Solaris)

Obtaining the Installation Program (Solaris)

VA Publisher is distributed on a CD. Install it from the CD.

Installing from a CD

To install VA Publisher from a CD

- Step 1 Insert the CD into the CD drive on your intended VA Publisher server.

- Step 2 Install the VA Publisher in a similar fashion to how you install other Solaris software packages. For information on packages, refer to the **pkgadd**, **pkginfo**, and **pkgrm** UNIX online reference manual (man pages).

Installing VA Publisher (Solaris)



NOTE: To add a package, you need to be logged in as “root” on the system where you are installing the package.

To install the VA Publisher

- Step 1 To extract the VA Publisher package from the tar archive enter the following from the directory where you downloaded the `VCpub.tar` file:

```
tar -xvf ./VCpub.tar
```

- Step 2 Log on as “root” on the machine where you want to install the VA Publisher.

- Step 3 Open a shell window and enter the following at the command prompt:

```
pkgadd -d .
```

The **pkgadd** menu appears.

- Step 4 Type 1 [ENTER] to select **VCpub** as the package you want to install. The software license agreement is displayed.



NOTE: For the remainder of this installation script: y=Yes, n=No, ? = Help, and q=Quit. Press [ENTER] alone to accept the default value.

- Step 5 Type y [ENTER] to accept the terms of the software license agreement.
A user prompt message is displayed - “Are you accessing the external publisher through a proxy server?”

Step 6 Type y [ENTER] to select **VCpub** as the package you want to install.
The license agreement is displayed.

Step 7 Type y [ENTER] for yes, or n [ENTER] for no.
If you typed y [ENTER] then you must type the
proxyservname[ENTER], and *portnumber*[ENTER] when prompted.
The following menu displays:

Select the type of CA you are using (Default LDAP):

Choose 1 (LDAP) for following CA's:

- Netscape CMS 4.0 and later,
- GTE CyberTrust Enterprise CA,
- Entrust/PKI 4.0d and later,
- Baltimore UniCERT w/ LDAP Directory,
- Any other CA storing CRLs in an LDAP Directory.

Choose 2 (HTTPS) for Netscape Certificate Server 1.x

Choose 3 (HTTP) for VeriSign OnSite

Or 4 (File) for:

- Baltimore UniCERT,
- Any other CA storing CRLs in a file

- 1 LDAP
- 2 HTTPS
- 3 HTTP
- 4 File

Enter selection (default: LDAP) [?,??,q]:

For LDAP installation go to step 8

For HTTPS installation skip to step 10

For HTTP installation skip to step 12

For FILE installation skip to step 14

LDAP Installation Path

Step 8 Type 1 [ENTER].

The following install script is displayed. Type responses that apply to your installation. To accept a default value press [ENTER].

Where do you want to install the VA Publisher?

Default: /usr/local/valicert/ [?,q]

Enter the name of the LDAP server:

Enter the LDAP server's port number:

Enter the DN containing your CRL. [?,q]

Enter the attribute for the CRL under the <DNname> DN.
[?,q]

Select the encoding of the CRL:

- 1 base64
- 2 der
- 3 hex

Enter selection (default: base64) [?,?,q]:

Enter the name of your validation server:
Default: perf-sun-2 [?,q]

Enter the port number of the validation server:
Default: 80 [1-33333,?,q]

Do you want to continue with the installation of <VCpub>
[y,n,?]

Step 9 Type y [ENTER].

The VA Publisher installation on a Sun Solaris workstation is completed. You are now done with this chapter.

HTTPS Installation Path

Step 10 Type 2 [ENTER].

The following install script is displayed. Type responses that apply to your installation. To accept a default value by press [ENTER].

Enter the absolute path of the directory that contains your Netscape Certificate Server instances. [?,q]

The following Netscape Certificate Server instances have been found on your system:

- 1 serverinstance-1
- 2 serverinstance-2

#comment: these server instances will be different for

```
#your installation.

Enter selection [?,??,q]:

Enter the port number for Certificate Server Instance:
Default: 443 [?,q]

Enter the name of your validation server:
Default: valserver [?,q]

Enter the port number of the validation server:
Default: 80 [1-33333,?,q]

Do you want to continue with the installation of <VCpub>
[y,n,?]
```

Step 11 Type y [ENTER].

The VA Publisher installation on a Sun Solaris workstation is completed. You are now done with this chapter.

HTTP Installation Path

Step 12 Type 3 [ENTER].

The following install script is displayed. Type responses that apply to your installation. To accept a default value press [ENTER].

```
Where do you want to install the VA Publisher?
Default: /usr/local/valicert [?,q]

Enter the name of your validation server:
Default: valserver [?,q]

Enter the port number of the validation server:
Default: 80 [1-33333,?,q]

Do you want to continue with the installation of <VCpub>
[y,n,?]
```

Step 13 Type y [ENTER].

The VA Publisher installation on a Sun Solaris workstation is completed. You are now done with this chapter.

FILE Installation Path

Step 14 Type 4 [ENTER].

The following install script is displayed. Type responses that apply to your installation. To accept a default value press [ENTER].

Where do you want to install the VA Publisher?

Default: /usr/local/valicert [?,q]

Please specify the absolute path for the file containing the CRL? [?,q]

Enter the name of your validation server:

Default: valserver [?,q]

Enter the port number of the validation server:

Default: 80 [1-33333,?,q]

Do you want to continue with the installation of <VCpub> [y,n,?]

Step 15 Type y [ENTER].

You have now successfully completed the VA Publisher installation on a Sun Solaris workstation.

CHAPTER 4

Using Certificate Servers

This section describes how to use VA Publisher with a variety of certificate authorities and other data repositories, including:

- ❖ Netscape Certificate Server (CMS v.1.1)
- ❖ Microsoft Certificate Server
- ❖ VeriSign CA
- ❖ CAs Using LDAP Directory Servers
 - Entrust/PKI
 - Baltimore UniCERT
 - GTE Cybertrust
 - and others
- ❖ File-Based CRL Repository
- ❖ ValiCert VA

Table 4. Matrix of Actions

Data Sources and Destinations	Fetch Data	Publish Data
Netscape Certificate Authority	X	—
Microsoft Certificate Authority	X	—
VeriSign CA	X	—
CAs Using LDAP Directory Servers	X	X
File	X	—
ValiCert VA	—	X

Netscape Certificate Server (CMS v.1.1)

This section explains how to use VA Publisher to fetch a new CRL from the Netscape Certificate Server.

Interface Modes for Fetching CRLs

VA Publisher is invoked in two different ways:

- ❖ Native Interface — VA Publisher is invoked each time a new CRL is generated by the CA.
- ❖ LDAP Interface — VA Publisher fetches the CRL from the LDAP directory.

VA Publisher supports both the native interface and the LDAP interface when using CMS v1.01. When VA Publisher is used with CMS v4.x, only the LDAP interface is supported and VA Publisher fetches data from the LDAP directory. VA Publisher may be invoked at the command line. It may also be invoked as a service, so as to poll for a new CRL at fixed time intervals.

Table 5. Interface for CMS Version

CMS Version	Native Interface	LDAP Interface
v1.01	X	X
v4.x	—	X



NOTE: If you are using the LDAP interface, please refer to “CAs Using LDAP Directory Servers” on page 48.

After you install VA Publisher and restart your Netscape Certificate Management System (CMS), VA Publisher is automatically invoked by the CMS whenever it generates a new CRL. The Netscape CMS generates a new CRL when one of the following events occur:

- ❖ The CMS administrator revokes a certificate.
- ❖ The CMS administrator manually updates the CRL.

To set the CMS to revoke certificates

- Step 1 Use a Netscape browser to open the Certificate Management System's main page.
- Step 2 Click on the "Privileged" button in the left-hand frame.
- Step 3 Click on **Revoke Certificates** and follow the instructions on the subsequent web page.
After you confirm the revocation action, a pop-up box appears, providing the status of the transaction with the ValiCert VA Server.
- Step 4 If an error occurs, see Appendix A, "Testing and Troubleshooting."

To manually update the CRL

- Step 1 Use a Netscape browser to open the Certificate Management System's main page.
- Step 2 Click on the "Privileged" button in the left-hand frame.
- Step 3 Click on **Update Certificate Revocation List**.
- Step 4 On the subsequent page, make sure the **Update ValiCert Server** checkbox is enabled.
- Step 5 Click on the Update button.
After a moment, a pop-up appears, providing the status of the transaction with the ValiCert VA Server.
- Step 6 If an error occurs, see Appendix A, "Testing and Troubleshooting."

Microsoft Certificate Server

This section explains how to use VA Publisher to fetch CRLs from the Microsoft Certificate Server version 1.0/Windows 2000 CA.

Interface Mode for Fetching CRLs

VA Publisher only supports the Native Interface mode, with MS Certificate Server. In this mode, VA Publisher is invoked each time a new CRL is generated. VA Publisher can also be invoked manually, which causes it to fetch the CRL from a Microsoft Certificate Server. VA Publisher must be installed on the same machine as the Microsoft Certificate Server.

Revoking a Certificate

VA Publisher for Microsoft Certificate Server is invoked whenever the administrator of the Certificate Server revokes a certificate.

To revoke a certificate

Step 1 Open the Microsoft Certificate Server main page at:

`http://<host>:<port>/CertSrv`

Step 2 Click on the **Certificate Administration Log Facility** link.

Step 3 Select the certificate you wish to revoke.

Step 4 Click on the **Revoke** button.

Step 5 You must now generate a new CRL for use with VA Publisher.

Problem: Ideally, VA Publisher should also be invoked when a new CRL is published. However, the Microsoft Certificate Server APIs provided for this seem to have undocumented features or calls. As a result VA Publisher is not invoked when the Microsoft Certificate Server issues a new CRL.

Solution: You can work around this limitation by setting the `CA_GETNEWCRL` flag to 1 in the configuration file and running VA Publisher for the Microsoft Certificate Server from the command line.

Log File

To verify whether or not VA Publisher is working properly

- Step 1 Check the log file (by default called `vpublish.log`) in the installation directory
- Step 2 In case of error, see Appendix A, "Testing and Troubleshooting."

Testing with Microsoft Certificate Server and Microsoft Outlook

The Microsoft Certificate Server ships with a Default Policy Module that has the extension `KeyUsage` parameter set to `KeyExchange`. Microsoft Outlook 98 does not recognize certificates issued by Microsoft Certificate Server which contain the Default Policy Module. The ValiCert VA Publisher contains a policy module (`policy.dll`) for Microsoft Certificate Server that enables Microsoft Outlook 98 to work with certificates issued by the Certificate Server.

Installing Microsoft Certificate Server Modules

To install and register the certificate server trust policy module

- Step 1 Type the following from a command prompt:

```
prompt> net stop "certificate authority"  
prompt> regsvr32 <pathName>/policy.dll  
prompt> net start "certificate authority"
```

VeriSign CA

This section describes the publicly available CA hosting provided by VeriSign on the Internet, and how VA Publisher fetches the CRL from VeriSign.

Overview

Currently, the OnSite CA presents the CRL in the PKCS7 format while other CAs present individual CRLs in DER encoding.

Interface Modes for Fetching CRLs

When VA Publisher is installed, the default settings for the VeriSign CA are configured for the VeriSign OnSite CA only. However, if the user chooses to fetch CRLs from other Verisign Public CAs, refer to Chapter 5, "Customizing the VA Publisher."

To verify whether or not VA Publisher is working properly

Step 1 Check the log file (normally called `vpublish.log`) in the installation directory.

Step 2 In case of error, see Appendix A, "Testing and Troubleshooting."

However, since the size of an OnSite VeriSign CRL is huge, VA Publisher can be configured to check the CRL status (that is whether the CRL has changed since the last fetch).

CAs Using LDAP Directory Servers

This section describes how to use the ValiCert VA Publisher with an LDAP Directory Server, including:

- ❖ Entrust/PKI
- ❖ Baltimore UniCERT
- ❖ GTE Cybertrust
- ❖ and others

VA Publisher interfaces to LDAP directories. LDAP directories can be CRL sources, as well as destinations for published CRLs. VA Publisher can fetch a CRL from an LDAP directory, as well as update an LDAP directory.

LDAP Operation

VA Publisher supports LDAP Directory Server versions 2 and 3.

The LDAP version of VA Publisher can be invoked automatically — by the trigger mechanism of the LDAP directory. LDAP directories which do not support the trigger mechanism rely on either the manual mode or the continuous mode to invoke VA Publisher. VA Publisher must poll the LDAP directory whenever the current CRL is required.

To verify whether or not VA Publisher is working properly

Step 1 Check the log file (default name is `vpublish.log`) in the installation directory.

Step 2 In case of error, see Appendix A, "Testing and Troubleshooting."

By default during installation, VA Publisher is configured to fetch the CRL from a single node (attribute). However, VA Publisher can be configured to fetch data from multiple nodes in an LDAP directory. To do this, specify each node as a separate URL in the `LOCATION` variable of an input section of the `ini` file.

VA Publisher can be configured to publish to multiple nodes in an LDAP directory. To do this, specify each node in a separate output section of the `ini` file.

For more details on configuring VA Publisher, see Chapter 5, "Customizing the VA Publisher."

File-Based CRL Repository

There are two interfaces for file-based CRL repositories:

- ❖ Fetching the CRL from a file
- ❖ Publishing the CRL to a file

VA Publisher uses the File protocol to read and write from a file. It supports all the formats and encoding.

Fetching CRLs

By default, VA Publisher reads a single CRL from a file. In order for VA Publisher to read multiple CRLs, the CRLs must each be present in a different file and VA Publisher must be configured to read a CRL from each file.

Publishing CRLs

VA Publisher can be configured to publish to a file. If the specified file already exists, VA Publisher appends each newly received CRL to the end of the file.

ValiCert VA

VA Publisher can publish the CRLs to the ValiCert VA using the HTTP/HTTPS protocol.

Publishing CRLs

Currently the ValiCert VA accepts the CRL(s) from VA Publisher provided that the CRL is in the PKCS7 format, and is DER encoded. VA Publisher can be configured to publish to multiple VAs as well as the Global VA Service.

Customizing the VA Publisher

This chapter describes the ValiCert VA Publisher configuration file. Use this chapter as a configuration reference to customize the publisher.

Configuration File

The VA Publisher configuration file (`vpublisher.ini` by default) contains the variables used to configure and customize the publisher.

Backward Compatibility

VA Publisher version 3.2 ships with `ini` file version 2.0, but also supports previous versions of `vpublisher.ini` files (prior to `vpublisher.ini` file version 2.0).

Version 1.0 `vpublisher.ini` files must be edited to have `vpublisher.ini` file version 2.0 functionality.

Syntax

The general form for each line in the configuration file is:

```
PARAMETER = value
```

The `value` starts with the first non-whitespace character following the equal sign. A value enclosed in double quotes refers to a string variable such as a path. A line in the `vpublish.ini` file is ignored if:

- ❖ The `value` is missing.
- ❖ There is no '=' in the line.
- ❖ The line begins with a #.

Lines beginning with # are considered comments. The `ini` file contains section names which are enclosed in square brackets and have no corresponding value, for example `[INPUT_SECTION_1]`.



NOTE: Names of the configuration variables are case sensitive. The Windows NT environment is case insensitive but case retentive. Under NT if you set the environment variable `Dump_Config`, you might think that you are setting `DUMP_CONFIG`, but the VA Publisher does not see the assignment.

Variables

The ValiCert VA Publisher recognizes the variables listed in the following tables. To customize VA Publisher, edit or add the appropriate variables to your `ini` file. Some variables are optional and can be left out of your file.

Table 6. [VAPublisher] Master Section

Variable	Definition	Default Value
[VAPublisher]	The section name, which if present, indicates that this is a version 2 file. No section name indicates a version 1 file.	Mandatory for a Version 2 file.
VERSION	The version of the <code>ini</code> file, either 1 or 2. No version number indicates a version 1 file. This variable is mandatory to create a version 2 file.	Mandatory for a Version 2 file.
NUM_INPUT_LOCATIONS	The number of input sections in the <code>ini</code> file. Create an input section for each source of revocation data. This variable is a positive integer.	1, Mandatory
NUM_OUTPUT_LOCATIONS	The number of output sections in the <code>ini</code> file. Create an output section for each location where revocation data is published. It is a positive integer.	1, Mandatory
VC_LOG_FILE	The name of the log file. If this variable is not specified log files are created and are named with the prefix <code>VC_LOG_FILE_PREFIX</code> and a time stamp, for example <code><prefix><timestamp>.log</code> . When a log file reaches the size <code>MAX_LOG_SIZE</code> a new one is generated.	<code>./vpublish.log</code> , Optional

Table 6. [VAPublisher] Master Section (Continued)

Variable	Definition	Default Value
LOG_LEVEL	The level of detail for logging VA Publisher events: 0 for detailed logging or 1 for brief logging.	1, Optional
LOG_DIR	The directory where logs are stored.	./Logs, Optional
MAX_LOG_SIZE	The maximum size (in kilobytes) of a log file after which a new one is created.	1024, Optional
VC_LOG_FILE_PREFIX	The prefix which is prepended to log file names if VC_LOG_FILE is not specified.	pub, Optional
DEFAULT_PERIODICITY	The polling period for input (in minutes). This variable is a positive integer.	2, Optional
DEFAULT_FORMAT	The input data format, either <code>crl</code> , <code>cert</code> , or <code>pkcs7</code> .	<code>crl</code> , Optional
DEFAULT_ENCODING	The default input data encoding, either DER, HEX, or Base64.	DER, Optional
USE_CRL_STATE_STORAGE	This variable determines whether or not the publisher will store state information of revocation data. Possible values are 0, do not store state information or 1, store state information.	0, Optional
REQUIRE_RETRIES	This variable determines whether or not the publisher will re-try to fetch or publish revocation information if the source or destination is unavailable. Possible values are 0, do not retry or 1, retry.	0, Optional
DELTA_TIME_FOR_FETCH	The time interval (in minutes) after the CRL's Next Update elapses that VA Publisher fetches the CRL.	5, Optional
NUM_ON_ERROR_RETRIES	Number of times VA Publisher attempts to re-fetch or re-publish the data.	3, Optional
ERROR_RETRY_INTERVAL	The time interval (in minutes) between error retries.	5, Optional

Table 7. Microsoft Certificate Server Variables Only

Variable	Definition	Default Value
CA_CONFIGNAME	The name of the certificate server instance, e.g. if the certificate server is running on host INDUS and is called TestCA, this variable should be set to INDUS\TestCA. If this variable is not specified it is treated as localhost.	NULL, Optional
CA_CRLVALIDDAYS	If CA_GETNEWCRL is set to 1, this variable specifies the number of days that the new CRL is valid.	7, Optional
CA_GETNEWCRL	If set to 1, the certificate server generates a new CRL when queried for its CRL. Otherwise, the certificate server returns the existing CRL.	0, Optional

Table 8. Input Section—One for each Certificate Server

Variable	Definition	Default Value
[INPUT_SECTION_n]	Each input to VA Publisher requires an input section in the ini file. This variable is the name of the Input section. Allowable values of n are positive integers. There is no default value for this variable.	None, Mandatory
PERIODICITY	The periodicity of fetching data. If this variable not specified, it defaults to the DEFAULT_PERIODICITY value in the Master Section	None, Optional
VENDOR_NAME	Optional. Vendor name.	None, Optional
DUMP_CONFIG	The name of a file where the configuration dictionary is dumped. Used mainly for debugging. If this variable is not specified the configuration dictionary is not dumped.	None, Optional
PROXY_HOST	The name of host of the HTTP Proxy that sends the CRL to ValiCert Validation Authority (VA) Server outside the firewall. If this variable is not specified proxy delivery is not available.	None, Optional

Table 8. Input Section—One for each Certificate Server

Variable	Definition	Default Value
PROXY_PORT	The port number for the HTTP proxy server. If this variable is not specified proxy delivery is not available.	None, Optional
LOCATION	The location from where revocation data is fetched, specified as a URLs. The general format for this variable includes nine parameters listed below. [<format>;<encoding>;]<protocol>://[<userid>:<password>@]<host>[:<port>]/[<location>][/?<attribute>]. These parameters are described in the following table. To aggregate related data from multiple sources (for example to fetch a CRL and its cert) specify multiple LOCATION URLs on different lines.	None, Mandatory

Table 9. URL Parameters for the input LOCATION variable

Parameter	Definition	Default Value
format	The format of data fetched from this location. Allowable values are <code>crl</code> , <code>cert</code> , <code>pkcs7</code> , and are case insensitive. If this parameter is not specified the format defaults to the value of <code>DEFAULT_FORMAT</code> from the Master Section.	<code>DEFAULT_FORMAT</code> , Optional
encoding	The encoding of the data fetched form this location. Allowable values are <code>DER</code> , <code>HEX</code> , <code>BASE64</code> , and are case insensitive. If this parameter is not specified the format defaults to the value of <code>DEFAULT_ENCODING</code> from the Master Section.	<code>DEFAULT_ENCODING</code> , Optional
protocol	The protocol for data fetched from this location. Allowable values are <code>HTTP</code> , <code>HTTPS</code> , <code>LDAP</code> , <code>FILE</code> , <code>VALICERT</code> , <code>VALICERTS</code> , and are case insensitive.	<code>HTTP</code> , Mandatory
userid	This parameter is used for LDAP only. This is the user ID to authenticate to an LDAP database to fetch data.	None, Optional
password	This parameter is used for LDAP only. This is the password to authenticate to an LDAP database to fetch data.	None, Optional

Table 9. URL Parameters for the input LOCATION variable

host	The host for this location. If this parameter is not specified it defaults to <code>localhost</code> .	<code>localhost</code> , Optional
port	The port for this location.	80 for HTTP 443 for HTTPS 389 for LDAP, Optional
location	The location from where the revocation data is fetched.	LDAP - the CA DN, HTTP/S - the file location, FILE - the full file path, VALICERT/S, Microsoft - NULL, Optional
attribute	This parameter is used for LDAP only. This is the LDAP attribute for the LDAP protocol. VA Publisher will only fetch a CRL from the node specified by the DN and attribute. To fetch from multiple nodes, each must be specified as a LOCATION.	None, Optional

Table 10. Output Section—One for each Destination

Variable	Definition	Default Value
[OUTPUT_SECTION_n]	Each location that VA Publisher publishes to requires an output section in the <code>ini</code> file. This parameter is the name of the Output section. Allowable values of <code>n</code> are positive integers.	None, Mandatory
INPUT	This is a list of the input sources whose data is sent to this output destination. Each source is designated by the input section number. Separate multiple sources with semicolons. For example if this variable is defined as <code>INPUT = 2;3;7</code> data from [INPUT_SECTION_2], [INPUT_SECTION_3], and [INPUT_SECTION_7] is published to this destination.	None, Mandatory

Table 10. Output Section—One for each Destination (Continued)

Variable	Definition	Default Value
PERIODICITY	This variable specifies how often data is sent to the destination. If this variable is not specified it will default to the value of DEFAULT_PERIODICITY from the Master Section.	DEFAULT_PERIODICITY, Optional
LOCATION	The location where the revocation data is published specified as a URL. The general format for this variable includes the following nine parameters: [<format>;<encoding>;] <protocol>://[<userid>: <password>@]<host>[:<port>]/ [<location>][/?<attribute>]. The parameters are described in the following table.	None, Mandatory

Table 11. URL Parameters for the Output LOCATION variable

Parameter	Definition	Default Value
format	The format of data that is published to this location. Allowable values are <code>crl</code> , <code>cert</code> , <code>pkcs7</code> , and are case insensitive. If this parameter is not specified it defaults to the value of DEFAULT_FORMAT in the Master Section.	DEFAULT_FORMAT, Optional
encoding	The encoding of the data published to this destination. Allowable values are <code>DER</code> , <code>HEX</code> , <code>BASE64</code> , and are case insensitive. If this parameter is not specified it defaults to the value of DEFAULT_ENCODING in the Master Section.	DEFAULT_ENCODING, Optional
protocol	The protocol for data published to this destination. Allowable values are <code>HTTP</code> , <code>HTTPS</code> , <code>LDAP</code> , <code>FILE</code> , <code>MICROSOFT</code> , and are case insensitive.	HTTP, Mandatory
userid	This parameter is used for LDAP only. This is the user ID to authenticate to an LDAP database to publish data to the database.	None, Optional
password	This parameter is used for LDAP only. This is the password to authenticate to an LDAP database to publish data.	None, Optional
host	The host for this location.	localhost, optional

Table 11. URL Parameters for the Output LOCATION variable

port	The port for this location. The default value depends on the specified protocol.	80 for HTTP 443 for HTTPS 389 for LDAP, Optional
location	The location where the revocation data is published.	LDAP - the CA DN, HTTP/S - the file location, FILE - the full file path, VALICERT/S - NULL
attribute	This parameter is used for LDAP only. This is the LDAP attribute for the LDAP protocol.	None, Optional

Table 12. SNMP Section

Variable	Definition	Default Value
[snmp]	The section name for the Simple Network Management Protocol configuration section.	
pollafter	The frequency (in seconds) that the agent updates the MIB variables.	300, Optional
enableTrap	This determines whether the trap is on or not; 0 for off, 1 for on.	0, Optional
agentport	The port to which the agent sends traps. This variable applies to UNIX (Solaris) only.	10040, Optional
masterHost	The hostname of the SNMP Manager. This variable applies to UNIX (Solaris) only.	0, Optional
masterport	The port on which the Manager listens for the agent. This variable applies to UNIX (Solaris) only.	10040, Optional

Sample vpublish.ini File Before Editing

The following code is the current version of the `vpublish.ini` file, prior to editing:

```
#
# vpublish.ini template
#

#[VAPublisher] is the master section introduced in the version 2
configuration file
```

```
#If this section name were absent, it would mean that it is a
version 1 configuration file
#[VAPublisher]

#This VERSION variable is set to 2 to indicate it is a version 2
configuration file.
#If this is set version 1, it implies it's the version 1
configuration file.
#If this variable is absent, version of the configuration file
defaults to 1.
#VERSION

#The number of sections of type INPUT_SECTION_<n>
#NUM_INPUT_LOCATIONS

#The number of sections of type OUTPUT_SECTION_<n>
#NUM_OUTPUT_LOCATIONS

#The logging level. If this is set to 0 it implies debugging
logs
#If this is set to 1 it will log otherwise
#LOG_LEVEL

#The publisher will store all log messages into the following
file. Note that if this variable is not specified and
#The VERSION of the configuration file is greater than 1, then
the log messages will be stored in a directory
#with the rollover feature. It will not be stored in a single
file. For more details please look at the
#Following variables: LOG_DIR, VC_LOG_FILE_PREFIX, MAX_LOG_SIZE
#VC_LOG_FILE

#Takes effect only if the VC_LOG_FILE is not set and the VERSION
is greater than 1
#It is the directory under which the log files will be archived.
By default it is ./Logs
#LOG_DIR

#Takes effect only if the VC_LOG_FILE is not set and the VERSION
is greater than 1
#The format of the log file name is <prefix><timestamp>.log
#This variable sets the prefix in the log file name. By default
it is "pub"
#VC_LOG_FILE_PREFIX
```

```
#Takes effect only if the VC_LOG_FILE is not set and the VERSION
is greater than 1
#This specifies the maximum size of the log files after which
the log file will be rolled over
#The default size is 1024Kb
#MAX_LOG_SIZE

#The default periodicity for fetching crl per INPUT_SECTION_<n>
basis
#If the periodicity is specified in the INPUT_SECTION_<n>, it
will override
#the default periodicity only for that section
#DEFAULT_PERIODICITY

#The default format of the data fetched from different sources.
However the format
#If specified in the URL for the location of the data, will
override this default format.
#The possible values:
#1. CRL for certificate revocation list,
#2. CERT for certificates
#3. PKCS7 for collection CRLs and Certificates
#DEFAULT_FORMAT

#The default encoding of the data fetched from different
sources. However the encoding
#If specified in the URL for the location of the data, will
override this default format.
#The possible values:
#1. DER
#2. HEX
#3. BASE64
#DEFAULT_ENCODING

#If the proxy server is used, set the following variables.
#PROXY_HOST
#PROXY_PORT

#Use this variable only in case of using the HTTPS protocol for
fetching data from Netscape Certificate Server.
#Generate a HTML output displaying the status of submission of
data to various destinations
#By default internally it is set to 1 such that the status
report will be generated. The
#status reports are not generated if the publisher is running as
a service.
```

```
#Set this variable to 0 if the status report is not required in
non-service mode.
#GENERATE_REPORT

#Set this to 1 if the user wants to use this feature: stateful
fetching / publishing of data
#(Boolean, default 0, under the [VAPublisher] section
#USE_CRL_STATE_STORAGE

#Set these to 1 if the user wants to use this feature of
retrying if the connection fails
#for fetching from a server and publishing to server
#(Boolean, default 0, under the [VAPublisher] section)
#REQUIRE_RETRIES

#The time interval after the Next Update of the CRL is elapsed,
#should the publisher fetch the CRL again.
#In minutes (+ve INTEGER, default 5, under the [VAPublisher]
section) used only if USE_CRL_STATE_STORAGE is set.
#DELTA_TIME_FOR_FETCH

#Number of times the publisher should try sending the data
request to the source / destination
#(+ve INTEGER, default 3, under the [VAPublisher] section) used
only if REQUIRE_RETRIES is set
#NUM_ON_ERROR_RETRIES: (+ve INTEGER, default 3, under the
[VAPublisher] section) used only if REQUIRE_RETRIES is set

#At what time intervals should the publisher do the retries.
#In minutes (+ve INTEGER, default 5, under the [VAPublisher]
section) used only if REQUIRE_RETRIES is set
#ERROR_RETRY_INTERVAL

#Input Section
#-----
#This section will provide information of the location(s) from
where the publisher
#can fetch the data, the authentication information if required,
the format and encoding
#of the data fetched, the periodicity of polling at this
location and the protocol used
# to fetch this data
#[INPUT_SECTION_n] where n is any positive integer
#[INPUT_SECTION_1]
```

```
#The periodicity of fetching data from locations specified in
this section
#PERIODICITY

#Vendor name which is optional
VENDOR_NAME= "ValiCert"

#In the LOCATION variable, specify the information for the
location from where the data has to be fetched.
#Multiple such variables can be specified within this section.
It would imply that
#all the data from these multiple sections will be fetched and
submitted to the corresponding
#destination. As of now there does not exist any relationship
between these locations.
#It would be advised to have the locations for all CRLDPs
specified within the same section
#along with the location of delta CRL and full CRL if required
#
#Format of the URL specified as a value to the LOCATION
variable:
#[<format>:<encoding>:]<protocol>://[<userid>:<password>@]<host>
[:<port>]/[<location>][/?<attribute>]
#<format> can be PKCS7, CRL, or CERT
#<encoding> can DER, HEX or BASE64
#<protocol> can be HTTP, HTTPS, LDAP, FILE, VALICERT, VALICERTS,
Microsoft
#<userid>:<password> is the authentication information if
required to fetch the data
#<host>[:<port>] is the server details of which the port is
optional. The default port
#      will be used in accordance to the protocol. For
HTTP:80, HTTPS:443, LDAP:389
#<location> for the following protocols is specified below:
#      LDAP: the CA DN
#      HTTP(S) : the file location
#      FILE: the full file path
#      VALICERT(S), Microsoft : NULL
#<attribute> is the LDAP attribute to be used only in case of
the LDAP protocol
#LOCATION

#Output Section
#-----
#This section will provide information of the location(s) to
which the publisher
```



```
#will publish data, the authentication information if required,
the format and encoding
#of the data to be published and the protocol used to publish
this data
#[OUTPUT_SECTION_n] where n is any positive integer
#[OUTPUT_SECTION_1]

#Specify the Input section number in this variable separated by
';'. For example INPUT=1;2
#The data from the fetched from the locations under the
specified input sections
#will be published to the location specified under this section
#INPUT

#In the LOCATION variable, specify the information of the
location to which the data is published.
# Only one instance of this variable can be used. Other
instances if specified will not considered.
#
#Format of the URL specified as a value to the LOCATION
variable:
#[<format>:<encoding>:]<protocol>://[<userid>:<password>@]<host
>[:<port>]/[<location>][/?<attribute>]
#<format> can be PKCS7, CRL, or CERT
#<encoding> can DER, HEX or BASE64
#<protocol> can be HTTP, HTTPS, FILE, VALICERT, VALICERTS
#<userid>:<password> is the authentication information if
required to fetch the data
#<host>[:<port>] is the server details of which the port is
optional. The default port
#           will be used in accordance to the protocol. For
HTTP:80, HTTPS:443, LDAP:389
#<location> for the following protocols is specified below:
#           HTTP(S) : the file location
#           FILE : the full file path
#           VALICERT(S) : NULL
#<attribute> is the LDAP attribute to be used only in case of
the LDAP protocol
#LOCATION

[snmp]
pollAfter=300
enableTrap=0
agentPort=10040
masterHost=localhost
masterPort=162
```

Sample Edited vpublish.ini File

The following code is an example of an edited vpublish.ini file:

```
#
# vpublish.ini template
#
[VAPublisher]
VERSION=2
NUM_INPUT_LOCATIONS = 1
NUM_OUTPUT_LOCATIONS = 2
LOG_LEVEL = 1

DEFAULT_PERIODICITY = 2
VC_LOG_FILE=my_log1.log

DEFAULT_FORMAT = CRL

DEFAULT_ENCODING = DER

USE_CRL_STATE_STORAGE = 1
REQUIRE_RETRIES = 1

[INPUT_SECTION_1]
PERIODICITY = 2

LOCATION=pkcs7;der;http://onsitecrl.verisign.com/OnSitePublic/
    LatestCRL

[OUTPUT_SECTION_1]
INPUT = 1

LOCATION = pkcs7;der;valicert://kosi.valicert.com:80

[OUTPUT_SECTION_2]
INPUT = 1
LOCATION = crl;der;file://out.txt

[snmp]
pollAfter=300
enableTrap=1
agentPort=10040
masterHost=localhost
masterPort=162
```

A

Testing and Troubleshooting

This section describes the methods to verify if VA Publisher is working properly.

Testing Tools

Tests can be used to see if the VA Publisher is operating correctly, such as writing CRLs to the output files using FILE protocol. (Use the SSLeay tools to test the CRL.)

For purposes of testing and troubleshooting, it is often useful to invoke the VA Publisher manually from a command shell. Using this test method, it may be helpful to configure VA Publisher, by setting some of the configuration variables on the command line, or by editing the configuration file. See Chapter 5, "Customizing the VA Publisher." for more information on command line options, and configuration variables.

An explanation of how to use testing tools is given in the following sections.

Testing with SSLeay Tools

You can use the SSLeay program to parse and test the various objects produced by VA Publisher or other parts of the system.

Testing the CRL Output

To examine the CRL produced by the VA Publisher in PKCS7 format

- Step 1 Set the configuration variable `PKCS7_FILE_OUT` to a file name (in this example, `test.pkcs7`).
- Step 2 Manually invoke the VA Publisher.
- Step 3 Run `ssleay` as follows to decode the contents:

```
Prompt> ssleay pkcs7 -in test.pkcs7 -inform DER -print_certs
```

The output should look something like this:

```

issuer= /C=US/O=ValiCert, Inc./OU=Applications/CN=Stefan
last update=Jun 4 01:42:25 1998 GMT
next update=Bad time value
-----BEGIN X509 CRL-----
MIIBajCB1DANBgkqhkiG9w0BAQQFADBOMQswCQYDVQQGEwJVUzEXMBUGA1UEChM
O
VmFsaUNlcnQsIEluYy4xFTATBgNVBAsTDEFwcGxpY2F0aW9ucuzEPMA0GA1UEAxM
G
U3RlZmFuFw05ODA2MDQwMTQyMjVaMGQwEgIBBBcNOTgwNDI5MTc0NTMyWjASAgE
I
Fw05ODA1MDEyMTMyNDdambICAQkXDtK4MDYwNDANNTI5NVowEgIBChcNOTgwNTA
3
MTcxMzMzMWjASAgELFw05ODA1MDCxNzI1NDl1aMA0GCSqGSIb3DQEBAUAA4GBALp
C
7p1+eJkK/SmNWCHEI59e++kECY4+KQplHSbwo7Tf1qUtKm93t53K1Zfmo8UF04q
O
LLqQtQG4Nh8FgBIU9Gq01eTheXzm9RO9VVDj05wv92g2tOt4Xe+dzaRM3ZDnl+4
m
vFOLPGXeqn8bAmQE5rK/AvMAC7xAszFwv/ZPcap
-----END X509 CRL-----

```

Verifying CRL Contents

To confirm complete, correct, and accurate contents of the CRL

- Step 1** Copy the portion of the CRL text between the lines `BEGIN X509 CRL` and `END X509 CRL` inclusive, into a file (in this example, `x509.txt`).
- Step 2** Run `ssleay` using the following command to view the contents:

```
Prompt> ssleay asn1parse -in x509.txt
```

The output should look something like this:

```
0:d=0  hl=4  l= 362 cons: SEQUENCE
4:d=1  hl=3  l= 212 cons: SEQUENCE
```

```

    7:d=2  hl=2  l=   13 cons: SEQUENCE
    9:d=3  hl=2  l=    9 prim: OBJECT
:md5withRSAEncryption
   20:d=3  hl=2  l=    0 prim: NULL
   22:d=2  hl=2  l=   78 cons: SEQUENCE
   24:d=3  hl=2  l=   11 cons: SET
   26:d=4  hl=2  l=    9 cons: SEQUENCE
   28:d=5  hl=2  l=    3 prim: OBJECT           :countryName
   33:d=5  hl=2  l=    2 prim: PRINTABLESTRING :US
   37:d=3  hl=2  l=   23 cons: SET
   39:d=4  hl=2  l=   21 cons: SEQUENCE
   41:d=5  hl=2  l=    3 prim: OBJECT           :organizationName
   46:d=5  hl=2  l=   14 prim: PRINTABLESTRING :ValiCert, Inc.
   62:d=3  hl=2  l=   21 cons: SET
   64:d=4  hl=2  l=   19 cons: SEQUENCE
   66:d=5  hl=2  l=    3 prim: OBJECT
:organizationalUnitName
   71:d=5  hl=2  l=   12 prim: PRINTABLESTRING :Applications
   85:d=3  hl=2  l=   15 cons: SET
   87:d=4  hl=2  l=   13 cons: SEQUENCE
   89:d=5  hl=2  l=    3 prim: OBJECT           :commonName
   94:d=5  hl=2  l=    6 prim: PRINTABLESTRING :Stefan
  102:d=2  hl=2  l=   13 prim: UTCTIME           :980604014225Z
  117:d=2  hl=2  l=  100 cons: SEQUENCE
  119:d=3  hl=2  l=   18 cons: SEQUENCE
  121:d=4  hl=2  l=    1 prim: INTEGER           :04
  124:d=4  hl=2  l=   13 prim: UTCTIME           :980429174532Z
  219:d=1  hl=2  l=   13 cons: SEQUENCE
  221:d=2  hl=2  l=    9 prim: OBJECT
:md5withRSAEncryption
  232:d=2  hl=2  l=    0 prim: NULL
  234:d=1  hl=3  l=  129 prim: BIT STRING

```

Troubleshooting

Problem: CRL submission does not work

3 Possible Solutions:

- 1 Look in the `vpublish.log` file (accessible via the **Start** Menu) and check the error message against the following list:
- 2 “HTTP 403/Forbidden”: Your Enterprise VA does not have the root certificate for your CA installed

- 3 “Unable to convert PKCS7 object”: You are pointing to the wrong DN in your LDAP directory. Your `LDAP_CRL_ATTRIBUTE_FORMAT` setting is incorrect.

Problem: It takes a very long time for the Publisher to quit.

Solution: Verify that your `vpublish.ini` is pointing to the correct Enterprise VA address and port number.

Problem: I do not know if the CRL in my LDAP directory is bad, or the Publisher doesn't like it.

Solution: Copy the CRL to a disk file on the same machine as VA Publisher, and configure VA Publisher to read the CRL from the file.

Problem: Publisher fails on startup on Solaris and the following error message displays:

```
ld.so.1: ./vpublish: fatal: relocation error: file
./vpublish: symbol __1cH__CimplKcplus_init6F_v_:
referenced symbol not found Killed
```

Solution: The `libCrun.so.1` library does not include the symbol `__1cH__CimplKcplus_init6F_v_`. To fix, get the OS 5.7 shared library patch: 106327-06 for C++ at <http://sunsolve.Sun.COM/> which includes this symbol.

Problem: Arbitrary behavior of publisher with respect to scheduling of fetching and publishing of CRL when the stateful fetching and publishing flag is set.

Solution: Remove the `./src` and `./dest` directories which contain the state files.

The state files are corrupted as a result of permutation of the configuration of the sources and destinations. It is recommended that you delete these files each time the configuration file is changed.

B

Using the SNMP Agent

VA Publisher includes a Simple Network Management Protocol (SNMP) agent to help you monitor the VA Publisher through an SNMP Manager such as Hewlett Packard OpenView or IBM Tivoli.

This section contains information in the following categories:

- ❖ Requirements for SNMP
- ❖ Installation instructions
- ❖ Configuration
- ❖ MIB definitions

This section describes the setup needed to use the SNMP agent with VA Publisher on windows NT and Solaris.

Using SNMP with Windows NT

On NT, the SNMP agent runs as an extension to the native SNMP service. Make sure all the requirements are met, then install the VA Publisher SNMP Agent on the same machine as the VA Publisher host. To use the agent, load the MIBs at the SNMP manager.

Requirements for NT

- ❖ You must install the agent on the same host machine as the VA Publisher.
- ❖ You must have administrator access to the host.
- ❖ You must have the SNMP Service installed.



NOTE: To get the SNMP service, install Options Pack 4 (or greater). Then add the SNMP service. For further instructions consult your Microsoft Documentation.

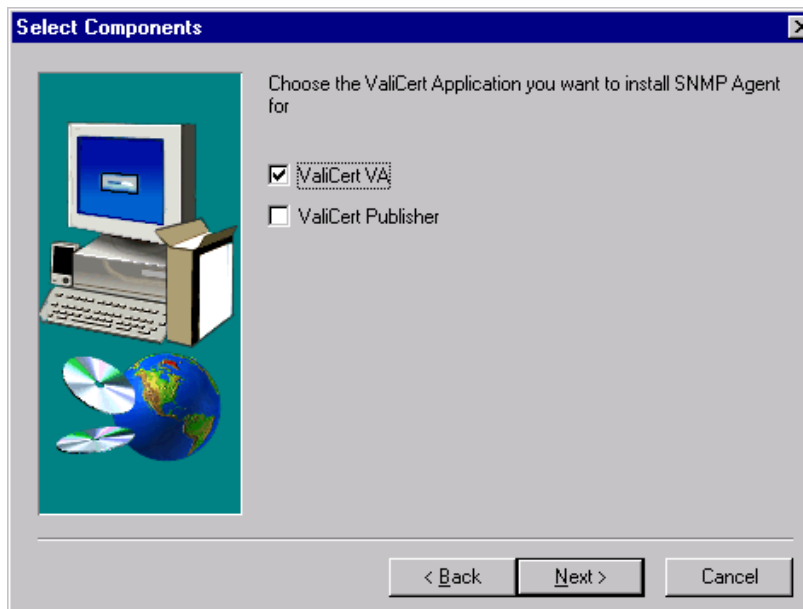
Installing the SNMP agent on Windows NT

To install the SNMP agent on NT, run the SNMP agent setup program. The program installs all the necessary components of the Agent.

To install the ValiCert VA Publisher SNMP Agent on Windows NT

- Step 1 Insert the CD containing the ValiCert VA Publisher into your CD-ROM drive.
- Step 2 Navigate to the SNMP folder.
- Step 3 Double-click on the self-extracting file SNMPAgent32Setup.
- Step 4 The Installation Folder dialog box displays.
Select a folder to extract the installation files into. If the folder does not exist you are prompted to create it.
- Step 5 Click **Finish**.
- Step 6 The installation files are unpacked and the Setup.exe program launches the installer.
The Install Shield application starts and the Welcome dialog box appears.
Follow the on-screen instructions as you proceed through the installation.
The **Next** button allows you to move forward to the next installation window.
The **Back** button allows you to return to the previous installation window
The **Cancel** button closes the installation program without installing any component of the VA Publisher SNMP Agent. To install VA Publisher SNMP Agent, rerun the setup program.
- Step 7 Click **Next**.
The ValiCert Software License Agreement dialog box appears:

- Step 8 Click **Yes** to accept the license agreement.
The Select Components dialog box appears:



- Step 9 Select the ValiCert Publisher checkbox.
- Step 10 Click **Next**.
The Agent installs and the Setup Complete dialog box displays
- Step 11 Select to display the README.
Select to start the SNMP agent.
- Step 12 Click **Finish**.

Using SNMP with UNIX (Solaris)

On UNIX, the SNMP agent runs as a `.tcl` script called `vaPubAgent.tcl`. The VA Publisher SNMP Agent is installed with the Publisher. To use the agent, load the MIBs at the SNMP manager.

Requirements

- ❖ You must have administrator access to the host.
- ❖ You must have scotty (the TCI/TK Extension for SNMP) installed.

Installing Scotty

If you do not have scotty, install it from the CD. The file is called `scottr.tar`. To install it type:

```
tar -xvf scotty.tar
```

Running the SNMP Agent for UNIX

To start the agent, at the prompt type:

```
scotty vaPubAgent.tcl
```

Configuring the SNMP Agent

To configure the SNMP agent (for Windows NT or for UNIX (Solaris) you must manually edit the file `valicert.ini` which is installed in the `entserv` directory of the VA Publisher installation. To do this open the file in a text editor and make the desired changes. below specifies the SNMP variables and their default values.

Windows NT

Traps and the ports used are native to the OS so no configuration of these is necessary. To set the polling period and turn on or off the traps edit the variables in the `ini` file.

UNIX (Solaris)

To specify the required host and port information and to enable traps edit the variables in the `ini` file.

SNMP Variables

The following are the SNMP variables contained in the `valicert.ini` file.

Table 1. SNMP Variables

Variable	Definition	Default Value
[snmp]	The section name for the Simple Network Management Protocol configuration section.	
pollafter	The frequency (in seconds) that the agent updates the MIB variables.	300, Optional
enableTrap	This determines whether the trap is on or not; 0 for off, 1 for on.	0, Optional
agentport	The port to which the agent sends traps. This variable applies to UNIX (Solaris) only.	10040, Optional
masterHost	The hostname of the SNMP Manager. This variable applies to UNIX (Solaris) only.	0, Optional
masterport	The port on which the Manager listens for the agent. This variable applies to UNIX (Solaris) only.	10040, Optional

MIB Variables

The following are the MIB variables used by the SNMP agent for the VA Publisher.

Regular

```
PUBLISHER-STATS-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        enterprises      FROM RFC1155-SMI
        DisplayString    FROM RFC1213-MIB
        OBJECT-TYPE      FROM RFC-1212;
    valicert             OBJECT IDENTIFIER ::= {enterprises 2930}
    SNMP                 OBJECT IDENTIFIER ::= {valicert 5}
    publisher            OBJECT IDENTIFIER ::= {SNMP 1}
    stats                OBJECT IDENTIFIER ::= {publisher 1}
    --
    *****
    *****
```

```
MibRevMajor OBJECT-TYPE
    SYNTAX  INTEGER (1..65535)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The major revision level of the MIB.
        This value tracks major functional changes made to the
MIB."
    ::= { stats 1 }

MibRevMinor OBJECT-TYPE
    SYNTAX  INTEGER (0..65535)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The minor revision level of the MIB.
        This value tracks minor changes made to the MIB."
    ::= { stats 2 }

PublisherVersion OBJECT-TYPE
SYNTAX  DisplayString (SIZE (1..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "VA Publisher's version string
        This string value indicates the VA Publisher's version
number."
    ::= { stats 3 }

PublisherIniVersion OBJECT-TYPE
SYNTAX  DisplayString (SIZE (1..255))
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "VA Publisher's version string
        This string value indicates the VA Publisher's version
number."
    ::= { stats 4 }

MemoryUsed OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
        "The amount of system memory the VA Publisher process
is currently using."
```

```
 ::= { stats 5 }

LastErrorMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (1..2048))
ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The latest ERROR message from the VA Publisher"
 ::= { stats 6 }

LastWarningMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (1..2048))
ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The latest WARNING message from the VA Publisher"
 ::= { stats 7 }

LastInfoMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (1..2048))
ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The latest INFORMATION message from the VA
Publisher"
 ::= { stats 8 }

LastDebugMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (1..2048))
ACCESS read-only
STATUS mandatory
DESCRIPTION
    "The latest DEBUG message from the VA Publisher"
 ::= { stats 9 }

END
```

Trap

```
VA-PUBLISHER-TRAPS-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        enterprises      FROM RFC1155-SMI
        DisplayString     FROM RFC1213-MIB
        OBJECT-TYPE       FROM RFC-1212
        TRAP-TYPE         FROM RFC-1215;
```

```
valicert          OBJECT IDENTIFIER ::= {enterprises 2930}
SNMP              OBJECT IDENTIFIER ::= {valicert 5}
server           OBJECT IDENTIFIER ::= {SNMP 2}
publisher        OBJECT IDENTIFIER ::= {SNMP 1}
traps            OBJECT IDENTIFIER ::= {publisher 2}
--
*****
*****

Major            OBJECT-TYPE
                SYNTAX  INTEGER (1..65535)
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                "The major revision of the MIB

                Major."
                ::= { traps 1 }

Minor            OBJECT-TYPE
                SYNTAX  INTEGER (0..65535)
                ACCESS  read-only
                STATUS  mandatory
                DESCRIPTION
                "The minor revision of the MIB  Minor"
                ::= { traps 2 }

-- Traps

PublisherIsDown  TRAP-TYPE
                ENTERPRISE traps
                DESCRIPTION
                "VA Publisher is down."
                ::= 50

END
```

Index

A

- abbreviations and acronyms ix
- Acronyms ix
- architecture 10
- arguments 11
- audience vii

B

- backward compatibility 51
- Baltimore UniCERT 3
- Base64 5

C

- CA vendors, multiple 3
- certificate authorities
 - list of supported 43
 - matrix of actions 43
- Certificate Authority 1
- certificates
 - revoking 45
 - revoking for MS Certificate Server 46
- command line 10
- command line arguments 11
- Command Line Mode
 - Mode 10
- configuration 12
- configuration file 51
- configuring
 - LDAP on UNIX 35
 - Netscape CMS on UNIX 36
- continuous 10
- Continuous Mode

Mode 10

- continuous mode 10
- conventions, typographical viii
- credits, other products used x
- CRL 1
- CRLDP 4
- CRLDPs 1
- CRLs
 - fetching 44, 50
 - file-based repositories 49
 - manually updating 45
 - publishing 50
 - testing output 65
 - verifying contents 66

D

- daemon 6
- data formats 4
- Default Policy Module 47
- definition of terms ix
- DER 5
- Destination Folder dialog box 21
- destinations, multiple 4
- document set ix

E

- encoding 4
- encodings 4
- Enterprise VA 69, 71
- Entrust PKI 3
- EVA30Setup package 70
- events 6

F

- features 3
- fetch 6
- fetching
 - CRLs 44
 - protocols 5
- FILE
 - installation path 41
- File source type 4
- file-based CRL repositories 49
- full CRL 4
- full CRLs 1

G

- glossary ix
- GTE 3

H

- HEX 5
- HTTP
 - installation path 40
- HTTPS 5
 - installation path 39

I

- input data types 1
- installing
 - Enterprise VA (NT) 69, 71
 - modules 47
 - procedure 70
 - VA Publisher 17
- installing (NT) 69, 71
- installing on UNIX 36
 - FILE nstallation path 41
 - HTTP installation path 40
 - HTTPS installation path 39
 - LDAP installation path 38
- interface modes 44

L

- LDAP 5
 - installation path 38
 - operation 49
- LDAP Directory 3, 4
- LDAP Directory Server
 - using 48
- LDAP interface 44
- LDAP servers 1
- log file 47

- log file, default 6
- logging
 - events 6

M

- MIB 7
- Microsoft CA 3
- Microsoft Certificate Server
 - installing modules 47
 - inteface modes 46
 - revoking certificates 46
- modes of operation 10

N

- native interface 44
- Netscape CA 3
- Netscape Certificate Management System
 - see Netscape CMS
- Netscape CMS
 - obtaining root certificate 14
 - revoking certificates 45
 - using 44
- Netscape Communications x
- note, explanation of viii

P

- PKCS7 4, 6, 65
- policy.dll 47
- pre-installation tasks 14, 34
- privileges 14, 34
- protocols, fetching data 5
- publish 6

R

- revoking
 - certificates for MS Certificate Server 46
- RSA Data Security x

S

- service 6
- SNMP 7
- source types 3
- SSLeay software x
- SSLeay Tools 65
- state information 2
- support
 - getting technical assistance x
- symbols viii

system requirements 14, 34

T

technical support x

testing tools 65

triggered 10

Triggered Mode

Mode 10

triggered mode 12

troubleshooting 67, 69

typographical conventions viii

U

upgrading

UNIX 34

Windows NT 14

V

VA Publisher

architecture 10

backward compatibility 51

command line arguments 11

configuration 12

configuring

Netscape CMS 36

configuring LDAP 35

customizing 51

destinations 1

features 3

installing 17

invoking 11

modes of operation 10

operation 9

testing tools 65

troubleshooting 67

upgrading 14, 34

using Netscape CMS 44

ValiCert Enterprise VA 3, 4

ValiCert Global VA Service 1, 3, 4

ValiCert VA

publishing CRLs 50

using 50

VA Publisher destination

ValiCert VA Publisher

installing on UNIX 36

ValiCert Validation Authorities

See ValiCert VA

validation authority

See ValiCert VA

VCpub.tar file 37

VeriSign Onsite CA

interface modes 48

source type 3

using 47

vpublish.ini file

sample 58

syntax 51

W

Windows NT

installing Enterprise VA 69, 71

X

X.509 Certificates 1

X.509 certificates 1, 5

